# PAIKALLISESTA VIDEOVALVONTAJÄRJESTELMÄSTÄ ”ÄLYKKÄÄKSI” VERKKOPOHJAISEKSI KAMERAVALVONTAJÄRJESTELMÄKSI

10. Turvallisuusjohdon
koulutusohjelma
Teknillinen korkeakoulu
Koulutuskeskus Dipoli
Tutkielma 3.1.2010
Eero Pelkonen

# Sisällysluettelo

# 1. Johdanto

Videovalvontajärjestelmien läpimurto valvontakäyttöön tapahtui 1980-luvun alkupuolella, jolloin mm. musta/valko CCD-kennolliset kamerat tulivat markkinoille. Aluksi yksittäisillä kameroilla pyrittiin helpottamaan vaikeiden prosessien valvontatehtävien hoitamista, mutta myös saamaan tehokkuutta prosesseihin. Tällöin jo rakennettiin teollisuuden ensimmäiset suuremmat prosessien videovalvontajärjestelmät. Tämän jälkeen videovalvonta alkoi yleistyä valvontakäytössä sekä viranomaistaholla että yksityisissä kohteissa. Tuolloin kaikki järjestelmät rakennettiin ns. paikallisiksi, ja näin ollen myös kuvavalvomot ovat olleet kiinteästi osana tuota paikallista valvontajärjestelmää. Teollisuuden prosessivalvonnassa ei alkuaikana käytetty kuvantallennustekniikkaa ollenkaan, vaan kamerat ja monitorit olivat vain helpottamassa monimutkaisten, olosuhteeltaan vaikeiden ja osittain jopa vaarallisten prosessin eri osien valvontaa. Videovalvonta ja yleensäkin valvomotyöskentely oli tuolloin työvoimavaltaista toimintaa, mutta jo silloin saatiin kustannussäästöjä, kun verrataan, että kaikki se valvonta olisi toteutettu prosessipisteittäin henkilötyötunteina.

Tilanne 1980-luvulta nykypäivän on muuttunut niin tuotantovaatimusten, -laadun kuin –kustannustenkin osalta radikaalisti. 80-luvun tekniikan mukaan rakennettuja järjestelmiä on vielä runsaasti niin teollisuuden, kaupanalan kuin viranomaistenkin käytössä. Yhteiskunnan muuttuminen, kilpailun kovenemien ja tuotantovaatimusten kasvamien ovat pakottaneet yritykset ja valtionhallinnon keskittämään ja rationalisoimaan kaikkia toimintoja rajusti. Tästä on syntynyt suuria tarpeita kehittää mm. videovalvontajärjestelmiä, valvomotoimintoja ja näiden em. asioiden palveluja. Valvomotoimintojen kehittyminen ja keskittäminen mahdollistaa myös muiden turvallisuusjärjestelmien informaation keskittämisen. Tämän päivän TCP/IP- tekniikka mahdollistaa eri sovellutuksilla modifioida tuon ajan tekniikan vielä ”älykkääksi” verkkopohjaiseksi kameravalvontajärjestelmäksi, jossa on mahdollista sekä keskittää kuvainformaation tallennusmahdollisuus että kohteiden etävalvonta.

## 1.1. Tavoitteet ja rajaus

Tutkielmassa ei ole tarkoitus selvittää tarkkaan videovalvontajärjestelmän laitteita ja niiden toimintaa. Tutkielmassa keskitytään esittämää järjestelmien käytettävyyttä, tekniikan tuomia ”älykkyys” mahdollisuuksia erilaisten anturoiden avulla, uusia valvontaomi-

naisuuksia ja nykyaikaisen TCP/IP-tekniikan antamia mahdollisuuksia keskittää toimintoja etävalvomoihin. Tavoitteena on esittää tekninen ratkaisumalli esim. suuren suomalaisen teollisuuden konsernille, jolla on useita toimipisteitä Suomessa ja tuoda esiin valvomotoimintojen keskittämisellä saavutettavat kustannussäästöt. Näiden toimintojen toteuttaminen vaatii tiettyjä teknisiä toimenpiteitä, jotta etävalvonta olisi mahdollista, ja että ennen kaikkea siitä saatava hyöty vastaisi asetettuja tavoitteita paikallisen valvomotoiminnan toimintojen supistumisen tai lakkauttamisen jälkeen.

Tässä tutkielmassa ei käsitellä järjestelmien omistussuhteeseen liittyviä yksityiskohtia. Järjestelmät voi omistaa joko asiakas tai palveluntoimittaja.

### 1.2. Tutkielman aineisto ja sisältö

Tämän tutkielman aineisto käsittelee kameravalvontajärjestelmän peruskomponentteja ja lisäksi järjestelmälle muita lisäarvoa tauottavia komponentteja, joilla saadaan lisää ”älyä” kameravalvontajärjestelmään. Yhtenä keskeisenä asiana ovat nykypäivän verkkotekniikan antamat mahdollisuudet kameratekniikan ja kuvavalvonnan keskittämisessä, sekä saatavat hyödyt niin kustannustasoon kuin myös valvonnan kattavuuteenkin nähden. Tutkielmassa käsitellään myös kuvavalvonnan TCP/IP-pohjaista turvaverkkojärjestelmää ja sen turvallisuutta. Tutkielman aineisto perustuu pitkälti alan ammattilaisten haastatteluun ja omiin kokemuksiin turvallisuusjärjestelmien - ja palvelukokonaisuuksien suunnittelusta.

## 2. Lainsäädäntö

Kameravalvontajärjestelmiä on rakennettu paljon ennen kuin lainsäädäntö on ehtinyt rajoittamaan, ohjeistaan tai opastamaan niiden käyttöä. Viimeisten vuosien aikana, kun lainsäädäntö on ollut voimassa, on yrityksissä ja laitoksissa tehty lain vaatimia korjauksia. Mielestäni tilanne valvontakohteissa on lain vaatimassa kunnossa.

Kameravalvontaan liittyvä lainsäädäntö on tällä hetkellä varsin pinnallinen ja siitä ei ole yhtä omaa lakia. Viimeisimmät lait, jotka säätelevät kameravalvontaa ovat varsin uusia ja näin niiden tuntemus ei ole vielä kaikilta osin teknistä valvontaa suorittavien tiedossa. Kameravalvontaan liittyvät seuraavat lait: *Henkilötietolaki 22.4.1999/523*, *Rikoslaki*

*19.12.1889/39 ja Laki yksityisyyden suojasta työelämässä 13.8.2004/759.* **Liitteessä 1** em. lakien tärkeimmät kohdat, jotka liittyvät suoranaisesti kameravalvontaan.

Näkyvimmät puutteet teknisen kameravalvonnan toteuttamisessa ovat kameravalvonnasta ilmoittavien kilpien puuttuminen. Tallentavasta kameravalvonnasta ilmoittavissa kilvissä on myös usein puutteellinen merkintä, sillä niistä puuttuu yleensä sana ”tallentava”. Puutteita on myös henkilötietolain tarkoittamissa rekisteriselosteissa. Sama lienee tilanne laissa yksityisyyden suojasta työelämässä velvoitetun yhteistoiminta – ja kuulemisvelvoitteiden suhteen. Aiheen käsittelyä hankaloittaa se tekijä, että teknistä valvontaa koskevan lainsäädännön soveltamisesta on tähän mennessä kertynyt hyvin vähän oikeustapauksia.

Suomessa kameravalvontajärjestelmiin liittyviä väärinkäytöksiä tulee esiin varsin vähän, vaikka järjestelmiä on asennettu runsaasti ja asennetaan jatkuvasti lisää.

## 3. Videovalvontajärjestelmien nykytila

Kokemukseeni perustuen videovalvontajärjestelmiä on rakennettu teollisuuden-, kaupanalan- ja viranomaiskäyttöön 1980-luvun loppupuolelta alkaen runsaasti. Tilanne 2000-luvulla on muuttunut eri toimialoilla hieman eriävästi toisistaan, koska järjestelmien käyttötapa ja -tarkoitus on varsin erilainen. Kaupan-alalla on siirrytty **multiplekseri** **[Sivu 38.]** ja nauhuripohjaisista tallenninjärjestelmistä lähes kokonaan digitaalitallenninpohjaiseen toteutustapaan.

Teollisuuden ja viranomaisten käytössä oleviin perinteisiin suuriin **videovaihdepohjaisiin** **[Sivu 38.]** ratkaisutapoihin kaupanalalla ei koskaan ole siirrytty suuressa mittakaavassa niiden kalliimman hankintahintaluokan takia. Teollisuus- ja viranomaiskäytössä on rakennettu ja rakennetaan edelleen videovaihdepohjaisia kameravalvontajärjestelmiä, joissa digitaalitallennintekniikka on vain lisäarvoa tuottava järjestelmä selvitettäessä prosessin toimintahäiriötä tai esim. rikoksiin liittyviä yksityiskohtia. Molemmat käytetyt tavat mahdollistavat nykypäivän tekniikan tuomilla mahdollisuuksilla toteuttaa keskitettyjä valvomoratkaisuja.

## 3.1 Yleisimmät kameratekniikat

Videovalvontajärjestelmien keskeisenä komponenttina ovat valvontakamerat. Kamerat ovat yleensä analogisia **CCD-kennolla** **[Sivu 38]** varustettuja värikameroita. Kameroiden CCD-kennon koko on yleensä 1/4” – 1”. Kameroiden ominaisuutena oleva yö/päivä-toiminto alkaa olla kohtuullisen yleinen malleista ja merkeistä riippumatta. Tällä toiminnolla tarkoitetaan sitä, että valaistuksen vähetessä kamera siirtyy musta/valko-tilaan. Tämän toiminnon avulla saadaan vielä noin 0,5 -0,7 luksin valaistuksessa tyydyttävää kuvan laatua. Kameroissa käytetyt optiikat ovat pääsääntöisesti auto-iiriksellä (automaattinen himmennin) varustettuja ja niiden aukkoluku F on 1.4 tai suurempi. Kameroiden valoherkkyys on yleensä luokkaa 1 lux.

Kaupanalan kohteissa kameroiden laatu on usein korvattu määrällä, joka näkyy parhaiten huonolaatuisena tunnistuskuvana normaali valaistuksessa ja kaupan yövalaistuksen aikana lähes tunnistamattomana tunnistuskuvana. Kameroiden laadun valintaan kaupanalalla on selkeänä syynä tiukka kilpailu markkinaosuuksista, jolloin valinta tehdään vain hinnan perusteella eikä laatua huomioida juuri lainkaan.

Teollisuuden ja viranomaistahojen käyttökohteissa on yleensä päädytty laadultaan huomattavasti korkeampaan tasoon kuin kaupanalalla. Käytettyjen kameroiden CCD-kennojen koko on yleensä jo ½”. Tähän ovat syynä olosuhteet (valaistus), sijoituspaikka, katseluetäisyydet jne. Teollisuus- ja viranomaiskohteissa kameroilta vaaditaan huomattavasti enemmän, koska ne muodostavat suuren osan tuotanto- ja aluevalvontaprosesseja. Kameroissa käytettävät optiikat ovat yleensä valoherkkyydeltään (F-luku on < 1.4) parempia ja ns. moottorizoomilla varustettuja, joten niillä pystytään katselemaan etäälläkin olevia kohteita kohtuullisen tarkasti. Teollisuus- ja viranomaiskäytössä kameroita sijoitetaan sekä kiinteästi että kääntyvälle alustalle eli kääntöpäälle.

Tämän päivän uusinta kameratekniikkaa on IP-kameratekniikka, jonka käyttö lisääntyy ns. yleisvalvonnassa. Tarkemmin IP-kameratekniikasta on esitetty kohdassa 4.4.

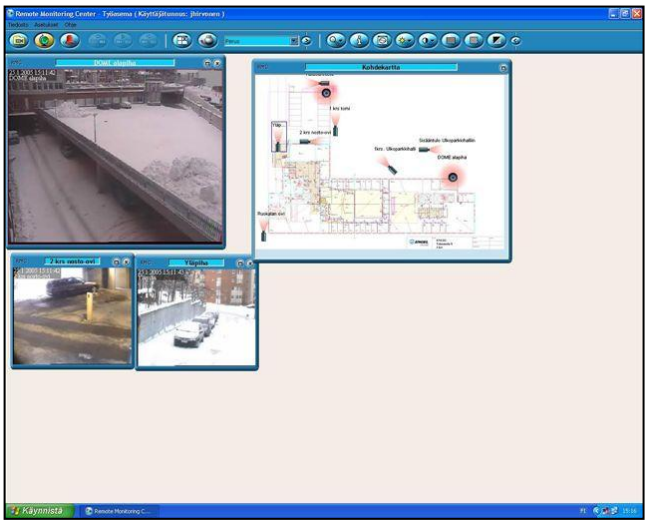
## 3.2 Yleisimmät valvomotekniikat

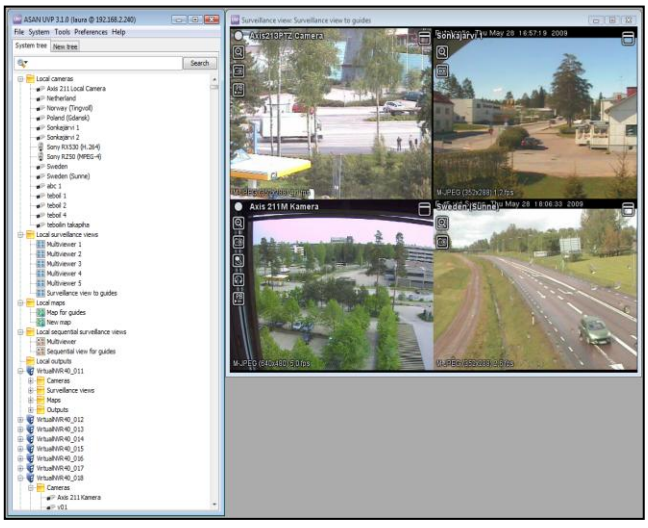
Tämän päivän valvomotekniikka perustuu selkeästi kahteen erilaiseen tekniikkaan.

- ohjelmalliset valvomotekniikat
- videovaihdepohjaiset valvomotekniikat

Ohjelmalliset valvomotekniikat ovat syntyneet vasta vuosituhannen taitteessa, jolloin digitaalitallennintekniikka löi itsensä läpi kuvantallennusmuotona. Ohjelmalliset valvomotekniikat mahdollistavat useamman digitaalitallentimen liittämisen ao. ohjelmaan. Ohjelmalla voidaan hallita kaikkien liitettyjen digitaalitallentimien kuvia ja mahdollisesti jopa ohjata kääntyviä kameroja. Digitaalitallentimiin voidaan liittää myös ulkopuolisia hälytysindikaatioita, jolloin tämä mahdollistaa esiasento-ohjattujen toimintojen toteuttamisen. Esimerkiksi varaston oven aukeaminen saa aikaan kameran kääntymisen ovelle ja kyseisen kameran kuvan siirtymisen valvomon näyttöön[9]. Esimerkkeinä tällaisista valvomo-ohjelmistoista ovat Mirasys Oy:n valmistama RMC-ohjelmisto (Remote Monitorig Center) ja ASAN Security Technologies Oy valmistama ASAN ASC (ASAN Surveillance Center). Alla olevissa kuvissa ovat työpöytänäkymät tällaisista valvomo-ohjelmista. Kuvista vasemmalla RMC ja oikealla ASAN ASC. Tällaisten ohjelmallisten valvomotekniikoiden käyttäjinä ovat tänä päivänä usein kaupanala ja tietysti viranomaistahot. Teollisuudessa näiden käyttö on vielä erittäin vähäistä.

Valvomo-ohjelmistoihin voidaan rakentaa kohteen karttapohjat ja niihin sijoittaa kameraikonit, joiden kautta ko kamerakuva saadaan avautumaan ja kamera saadaan hallintaan (kääntö-/zoom-toiminnot). Valvomo-ohjelmilla voidaan ohjata ulkopuolisia järjestelmiä esim. avata puomeja, portteja ja ovia tunnistuksen jälkeen. Työpöytä voidaan rakentaa käyttäjäkohtaiseksi eli kirjautumisen yhteydessä jokainen saa mieleisensä työpöydän käyttöoikeuksiensa puitteissa.





Videovaihdepohjaiset valvomot ovat 1980-luvun tekniikkaa, mutta puolustavat paikkaansa teollisuuden valvomoratkaisuissa vielä tänäkin päivänä. Videovaihdepohjaiset valvomot toimivat teollisuuden prosessivalvonnan kohteissa, joissa joudutaan jatkuvasti vaihtamaan / muuttamaan kameroiden kuvia monitorilta toiselle tai tekemään prosessin mukaan muuttuvia kuvakierroksia. Videovaihdepohjainen valvomotekniikka mahdollistaa suurten videovalvontajärjestelmien hallinnoinnin yhdestä valvomopisteestä. Tällaiseen suureen videovalvontajärjestelmään saattaa kuulua hyvinkin yli 1 000 kameraa ja useita kymmeniä valvontamonitoreja.

Valvomotekniikoita käytetään myös paljon yhdessä eli varsinainen operatiivinen toiminta tapahtuu ns. videovaihdepohjaisella järjestelmällä ja tarvittaessa historiatietoa tapahtuneesta, etsitä suoritetaan ohjelmallisella järjestelmällä. Viranomaiskäytössä tällaiset järjestelmät ovat hyvin yleisiä.

## 4. Kameratekniikan kehittyminen 2000- luvulla

Suurten kameravalmistajien kameroiden kehittyneimmät ja älykkäimmät ominaisuudet ovat peräisin 2000-luvun alusta. Parhaimmat analogiset kamerat saivat tuolloin mm. 15-bittisen näytteenoton ja XF-Dynamic-koneiston, joka laajentaa dynaamista aluetta. Tämä yhdistelmä tuottaa terävämmän ja tarkemman kuvan sekä erittäin hyvän värien toiston vaativissakin valaistusolosuhteissa. Analogisten huippukameroiden CCD-kenno on ½”, joka parantaa hämärässä kameran värientoistokykyä ja päivänvalossa kuvien terävyyttä[6].

Kameratekniikka kehittyy kovaa vauhtia IP-kameratekniikan saralla, koska digitaalisetverkot mahdollistavat yhä suurempien tietomäärien siirtämisen paikasta toiseen nopeasti ja varmasti. Analogikameratekniikka on taas ollut vähemmällä tuotekehityksellä viimeiset kaksi - kolme vuotta, koska sitä rajoittaa TV-standardit (PAL/NTS) ja toiseksi tiedonsiirtoverkot ovat mahdollistaneet IP-kameroiden käytön. Analogitekniikalla rakennettuja kameroja voidaan käyttää myös TCP/IP-pohjaisessa verkossa, kunhan analoginen kuvasignaali muutetaan digitaaliseksi A/D-muuntimella eli videopalvelimella.

## 4.1 Analogiset kamerat

Analogisien kameroiden ominaisuudet ovat kehittyneet huimasti viimeisten kymmenien vuosien aikana, jolloin vielä ei ollut näkyvissä voimakkaana IP-kameratekniikan tuleminnen[6]. Analogikameratekniikka puoltaa paikkansa niissä kohteissa missä tarvitaan varmaa ja erittäin hyvälaatuista kameratekniikkaa vaihtelevissa ja vaativissa olosuhteissa. Tämän kameratyypin käyttäjäkunta löytyy edelleen teollisuudesta ja viranomaistahoilta.

### 4.1.1 Ominaisuudet

Parhaimpien analogisten kameroiden ominaisuudet voidaan ilmoittaa muutamia vertailuarvoja käyttäen. Seuraavassa käytetyimmät analogisten kameroiden ominaisuuskriteerit ja niiden hyvää tasoa olevat arvot.

- kennon tyyppi ja koko — CCD-kenno, ½”
- erottelutarkkuus / vaakatarkkuus — 540 TV-juovaa tai enemmän
- herkkyys 50 IRE — 0,35 lux /0,14 lux (Night Sense)
- signaali-kohina-suhde — > 50 dB

Edellä kuvatuilla ominaisuuskriteereillä löytyy noin tusinan verran kameroita, jotka paperilla vertailtuina ovat lähes yhtä hyviä. Kohteessa suoritetulla käytännön kokeella varmistetaan ko. kohteeseen parhaiten soveltuva hinta / laatu-suhteeltaan oleva kamera.

Analogiakameratekniikan hyvät puolet[8]

- Standardin mukaiset laitteistot (PAL, NTSC)
- Mahdollistaa pidemmän yhtäjaksoisen siirtotien ja jatkuvan kuvan, 25 kuvaa/s
- Kamerat näkevät paremmin hämärässä (Herkkyys parempi)
- Automaattinen valaistuksen säätö kameroissa

Analogiakameratekniikan huonot puolet[8]

- Signaali herkempi sähköisille häiriöille (sähkö- ja magneettikentät)
- Tähtiverkko eli jokaiselle kamerapisteelle omat kaapelit -> kallis
- Tallentaessa tehtävä digitaalimuunnos, joka osin heikentää tallenteen laatuun
- Langattomuus vaatii tarkemmat tekniikan määritykset kohdekohtainsesti

### 4.1.2 Erottelukyky ja pimeänäkö ominaisuudet

Analogisten kameroiden ominaisuuksista tärkeimmät valintakriteeriin vaikuttavat tekijät ovat erottelukyky ja pimeänäköominaisuudet. Kameroiden erottelukyky on riippuvainen käytetystä CCD-kennosta ja sen koosta (1/4” – 1/2”). Käytetyimmät CCD-kennot ovat nykypäivänä 1/3” ja ½”. Näillä kennoilla saavutetaan vaakaerottelukyky joka vaihtelee 480 – 570 TV-juovan väliltä.

Analogikameroiden pimeänäköominaisuudet taas riippuvat käytetystä CCD-kennosta, sen koosta ja optiikasta. Lähtökohtana voidaan pitää sitä, että mitä suurempi CCD-kenno sitä parempi on pimeänäkökyky. Suurempi CCD-kenno kerää enemmän kohteesta tulevaa valoa kuin pienempi kenno. Optiikan tärkeä arvo: aukkoluku eli F on hyvissä ja valovoimaisissa optiikoissa jopa 1,0.

## 4.2 Dome-kameratekniikka

**Bosch VG4-Domekamerat**

Dome-kamerat eli PTZ-kamerat syntyivät 1980-luvun ja 1990-luvun taitteessa, jolloin ensimmäisiä kaupalliseen käyttöön soveltuvia dome-kameroita tuli myyntiin. Kameratekniikan kehittymisen syynä oli tarve saada vanhat ja hitaat kääntöpäät korvattua pienemmillä ja nopeammin kääntyvillä kameroilla. Toisekseen kauppaliikkeiden kameravalvonta vaati pienempiä ja huomaamattomampia kameroita, joilla voidaan valvoa huomaamattomasti. Näin syntyivät ensimmäiset ns. Flexi-domekamerat, joista myöhemmin kehittyivät varsinaiset domekamerat[6].

### 4.2.1 Ominaisuudet

Dome-kameroiden ominaisuuksista voidaan ilmoittaa samoja arvoja kuin perinteisistä analogikameroistakin, joita käsiteltiin kohdassa 4.1.1. Dome-kameroissa on lisäksi suuri joukko muita ominaisuuksia, joita ei ole tavallisissa kameroissa. Näitä ominaisuuksia on mm. automaattinen fokus-toiminto, jolloin kameraa käännettäessä kuva on koko ajan tarkka. Muita ominaisuuksia ovat mm. AutoTrack – liikkeenseurantaominaisuus, automaattisen liikkeentunnistusjärjestelmän kehittynyt **DSP-tekniikka** [sivu 38.], joka mahdol-

listaa videokuvan reaaliaikaisen käsittelyn ja siten erittäin tasaisen kohteiden seurannan. Sisäänrakennettu kuvanvakautus mahdollistaa pitkien polttovälien käytön pitkillä etäisyyksillä. Hälytysten käsittely on mahdollista suoraan kamerassa, jolla voidaan ohjata jopa ulkopuolisia laitteita. Kameran esiasento-ohjaus tukee kymmeniä esiasentoja ja useita ohjelmoituja valvontakierroksia. IP-luokitus mahdollistaa laajat käyttöolosuhteet vaativissa kohteissa (IP 66) ja laajan käyttölämpötila-alueen - 60 °C - + 55 °C[6].

Dome-kameroiden kehittyessä on niiden käyttö lisääntynyt erittäin voimakkaasti. Ne antavat vanhoille videovalvontajärjestelmille paljon uusia sovellutuksia ja valvontakohteita lisää. Ne ovat osittain syrjäyttämässä perinteistä kääntöpäätekniikkaa niiden paremman käytettävyyden ansiosta[6].

## 4.3 Lämpökameratekniikka


**Pelco lämpökamera kääntöpäällä**

**Bosch integroitu analogi- ja lämpökamera kääntöpäällä**

Lämpökameroiden käyttö on lisääntynyt aivan viime vuosina osana kameravalvontajärjestelmää. Tähän on ollut syynä suurten kameravalmistajien tuleminen näille markkinoille ja siitä seurannut voimakas hintojen lasku. Lämpökameroiden hinta oli kymmenisen vuotta sitten noin 200 000 euroa, jolloin lämpökameran investointipäätöksen tekeminen ei ollut helppoa. Nykypäivänä lämpökamera, joka pystytään liittämään kameravalvontajärjestelmään ja, jolla pystytään valvomaan kohteita aina noin 1 000 metriin saakka, maksaa noin 15 000 – 25 000 euroa. Lämpökameratekniikan kehittyessä jäähdytetyistä suurista kameroista on siirrytty pienempiin jäähdyttämättömiin malleihin, jotka voidaan helposti liittää osaksi kameravalvontajärjestelmää.

Uusimmat lämpökamera-sovellutukset ovat jo integroituja ratkaisuja normaalien kameroiden kanssa. Tällaisten integroitujen kokonaisuuksien hyvinä puolina voidaan pitää niiden pieniä fyysisiä ulkomittoja. Integroinnin huonona puolena on tietysti se, että molemmat kamerat sijaitsevat samassa kotelossa, joten vikatapauksissa koko järjestelmä on

irrotettava huoltoon ja näin ollen ko pisteessä ei ole valvontaa.

Lämpökameroiden saatavuudessa on tiettyjä rajoitteita ja luvanvaraisuuksia, joita mm. Yhdysvalloissa valmistettujen laitteiden osalta asettaa Yhdysvaltain puolustusministeriö. Luvanvaraisia lämpökameroita ovat sellaiset kamerat, jotka pystyvät tuottamaan täysin reaaliaikaista kuvaa. Tällaisellekin kameralle saadaan tuontilupa Suomeen, kunhan loppuasiakas täyttää tietyt kriteerit eli on jokin viranomainen ja ilmoittaa pitäytyvänsä myymästä laitetta kolmannelle osapuolelle. Lämpökamerat antavat vanhoille kameravalvontajärjestelmille paljon uusia sovellutuksia ja valvonta kohteita lisää.

### 4.3.1 Ominaisuudet

Lämpökameroiden ominaisuuksista voidaan ilmoittaa lähes samoja arvoja kuin perinteisistä analogikameroistakin.

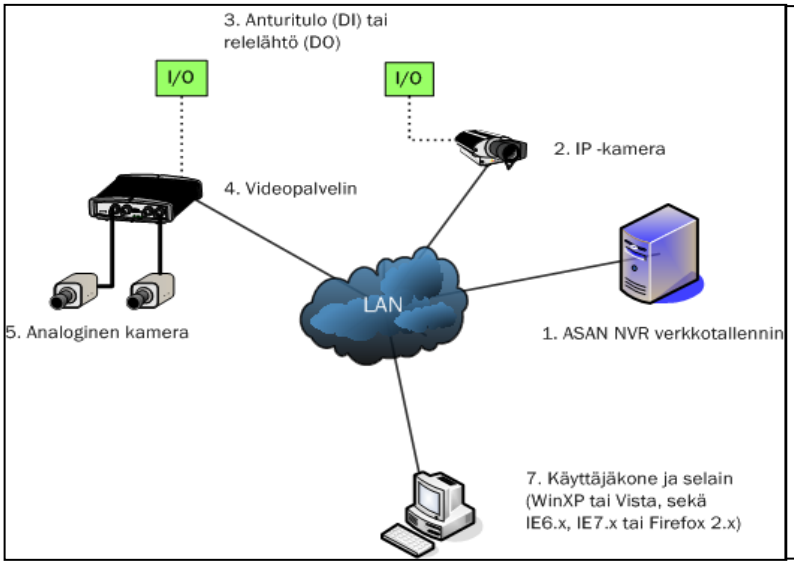
Lämpökameroita saadaan tänä päivänä sekä kääntöpäällä varustettuina että irrallisina sääsuojakoteloon asennettuina, jolloin lämpökamera voidaan helposti liittää jo olemassa olevan kameravalvontajärjestelmän kääntöpäähän. Lämpökameroita käytetään pääsääntöisesti vain suurteollisuudessa ja viranomaisten valvontakohteissa. Käyttökohteina ovat mm. aluevalvonnan ratkaisut, joilla pyritään seuraamaan alueella tapahtuvaa liikettä huonon näkyvyyden aikana, ja toisaalta seuraamaan teollisuuden tuotantoprosessien eri laitteiden lämpötiloja. Lisäksi uutena käyttökohteena ovat meripelastustehtävissä toimivat alukset.

## 4.4 IP-kameratekniikka

IP-kameratekniikka on jo yleistynyt terminä, jota käytetään kameroista, jotka voidaan liittää suoraan TCP/IP-verkkoon[3]. IP-kamerat ovat kehittyneet vasta viimeisen viiden vuoden aikana nykyiselle tasolle ja kehitys on edelleen voimakasta.

Periaatteena on, että yksittäiset IP-kamerat liitetään suoraan TCP/IP-verkkoon. TCP/IP-verkon kautta kuvat siirretään palvelutarjoajan palvelimelle tai yrityksen omassa hallinnassa olevalle keskitetylle palvelimeen[3]. Keskitetyn etävalvonnan palvelutarjoajat eivät mielellään hyväksy siirtotieksi yrityksen omaa tuotanto- tai toimistoverkkoa, koska tällöin verkon valvonta, hallinta ja sen toiminta eivät ole palvelutarjoajan kontrollissa. Mieluim-

min näissä tapauksissa käytetään ns. turvaverkkoratkaisuja, jotka on nimenomaan suunniteltu ja tarkoitettu turvallisuusjärjestelmien käyttöön. Alla olevassa kuvassa on yksinkertainen IP-kameraratkaisu[3].




1. Verkkotallennin (palvelin)
2. IP-kamera
3. Kärkitieto (DI) tai relelähtö (DO)
4. Videopalvelin, mahdollistaa analogikameroiden liittämisen
5. Analogiset kamerat
6. TCP/IP-verkko
7. Käyttäjäkone etäkatseluohjelmalla

Hinnaltaan IP-kamerat ovat vielä huomattavasti kalliimpia kuin perinteinen analoginen kameratekniikka. IP-kameroiden valoherkkyys on edelleen huonompi kuin analogikameroiden, joten ulkotilojen valvontaan ne soveltuvat vielä huonosti.

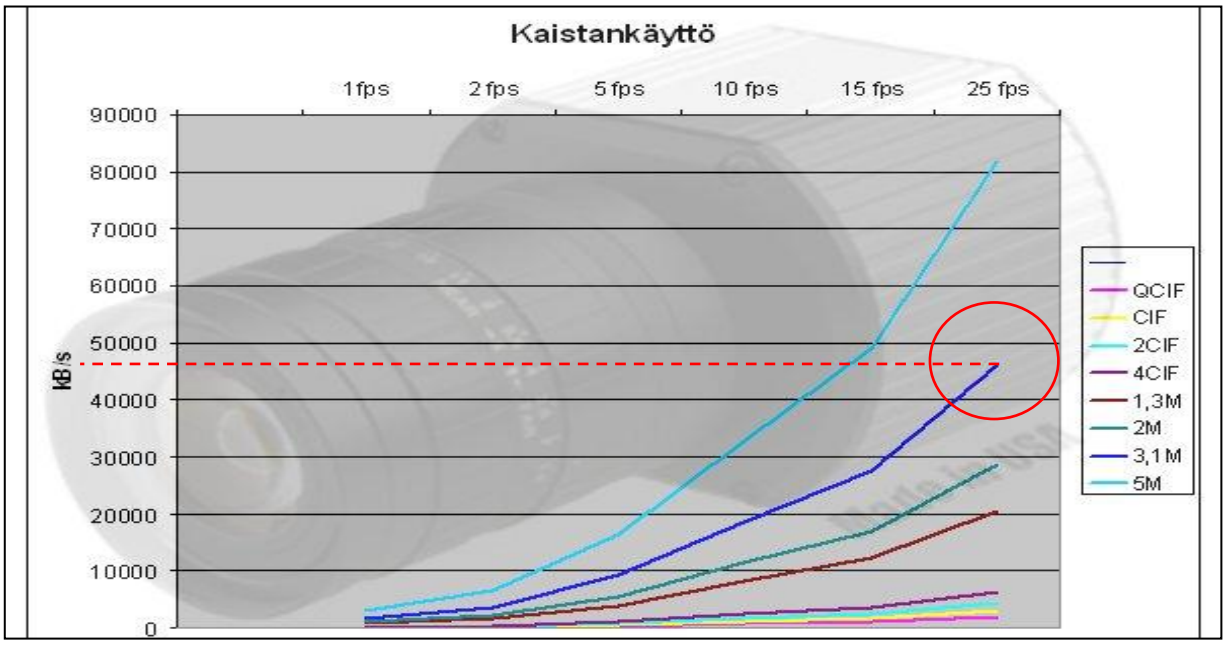
.

Esimerkinomaisesti tyypillisesti toimistorakennuksessa, saattaa olla 30 kappaletta hyvälaatuisia IP-kameroita, joista halutaan 4**CIF**[Sivu 38] kuvaa ja jokaisesta kamerasta 10 kuvaa/s. Tällainen kameramäärä em. ominaisuuksilla vaatii noin 300 Gb:n tallennuskapasiteetin vuorokautta kohden[1]. Nykypäivän digitaalitallentimilla tämä voitaisiin vielä juuri ja juuri toteuttaa ja saada kahden viikon tallennusaika. Suurella kuvatahdilla tallennettuja tapahtumia etsittäessä, kun ei tiedetä tarkkaa tapahtuma-aikaa, on varsin vaikeaa ja aikaa vievää toimintaa. Alla olevassa kuvassa on esitetty eri kuvakoot.

Aina ennen IP-kameroiden käyttöä tuotanto- tai toimisto-verkossa pitää käytettävissä oleva IP-verkko analysoija, jotta vältytään verkon ”kaatumiselta”, kun IP-kamerat on liitetty verk-koon. Alla esimerkkilaskelma em. kameramäärän mukaisesta verkkotarpeesta maksimikuormalla. Käytetään 4 CIF kokoista kuvaa, liike-tunnistus tapahtuu kamerassa, 10 kuvaa/kamera/s.

- Yksi kuva on 30 kB eli yksi kuva sekunnissa aiheuttaa kuormaa verkkoon
  30 kB/s = 30 x 1,024 x 8 bit/byte = **245,76 kbit/s**
- Halutaan katsoa kuvaa 5 fps ja tallentaa 5 fps, eli yhteensä 10 fps
  10 fps = 10 x 245,76kbit/s =**2457,60 kbit/s**
- Näitä kameroita on käytössä 30 kappaletta, jolloin **maksimikuorma** verkossa on:
  30 x 10 fps = 30 x 245,76kbit/s x 10 fps = **73,73 Mbit/s**[3]

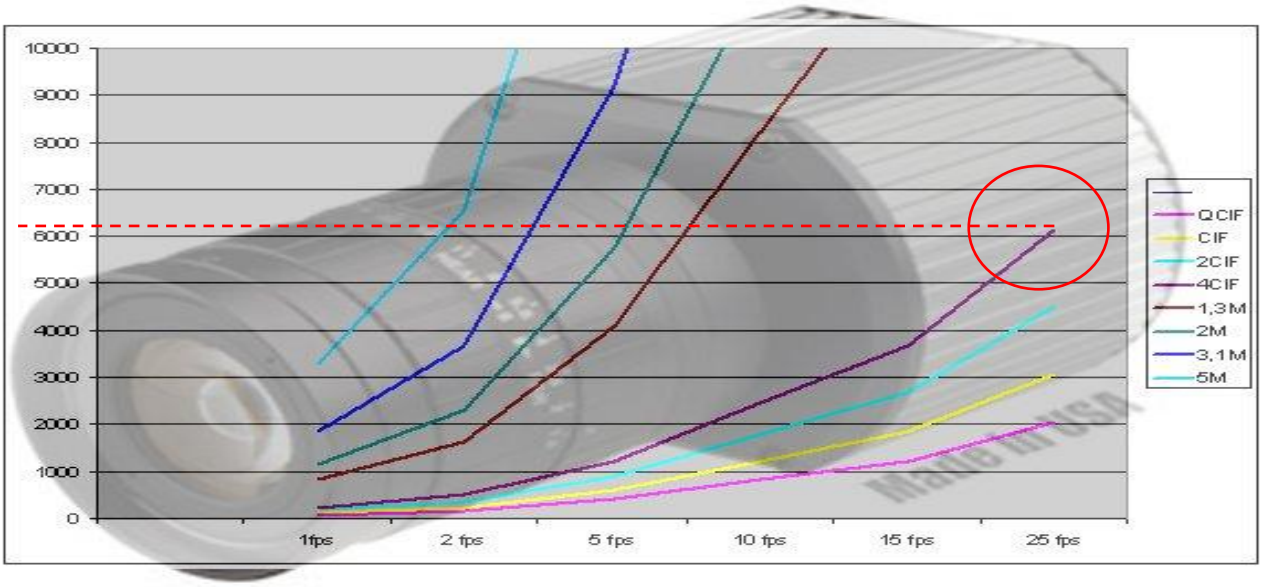
Em. laskelma osoittaa, että vaikka kohteessa olisi tätä kameramäärää varten varattu oma 100 Mbit/s verkko, niin verkon kapasiteetti riittäisi teoriassa juuri ja juuri. Käytännössä tuon 100 Mbit/s verkon todellinen kapasiteetti on noin vain 40 – 60 Mbit/s.




Edellisellä sivulla olevassa taulukossa on esitetty yksittäisen kameran tarvitsema verkkokaistan tarve. Taulukosta käy ilmi, että esim. 3,1 Mpix kamera, jonka kuvatahti on 25 kuvaa/s vaatii kaistaa noin 45 Mbit/s. Kaistantarve suhteessa kuvakokoon ja – nopeuteen kasvaa eksponenttiaalisesti[1].

Seuraavalla sivulla olevassa taulukossa tarkastellaan analogikameran tuottamaa 4 CIF kuvakokoa ja kuvanopeudella 25 kuvaa/s. Taulukosta nähdään, että kaistan tarve on

tällöin vain noin 0,6 Mbit/s[1]. Kaistantarve suhteessa kuvakokoon ja – nopeuteen (0-1Mitb kaistalla), MJPEG-pakkaustekniikalla




### 4.4.1 IP-kameroiden ominaisuudet

IP-kameroiden käyttö on yleistymässä. Seuraavassa on yhteenveto niiden hyvistä ja huonoista puolista.

IP-kameroiden hyvät puolet[8]

- **CAT5 / CAT6** [Sivu 38] kaapelointi datan siirtoon
- Infrastruktuuri yleensä jo olemassa (LAN verkko)
- Valmiiksi digitaalinen kuva ilman media muunnoksia, kuvan laatu hyvä
- Langatonta teknologiaa helpompi hyödyntää
  - Laajempi tuotevalikoima
  - Virheenkorjaus tiedonsiirrossa
  - Tietoturva parempi
  - GPRS / WLAN / WiMAX / @450 mobiili -verkot
- Hinnat tulossa alaspäin
- Keskitetty tallennus ja - valvonta toteutettavissa pienemmillä laite kustannuksilla
- Hyvissä valaistusolosuhteissa kuvanlaatu hyvä
- Vähemmän sähköisiä häiriöitä (magneettikenttä)
- Siirtotiet helpompi monistaa

IP-kameroiden huonot puolet[8]

- Etäisyysrajoitteet verkon alueella (n.100 m kytkimestä)
- Kaistan tarve siirtoverkossa (riippuu järjestelmän laajuudesta)
- Kameroiden herkkyys huonossa valaistuksessa, ei sovellu hyvin ulkovalvontaan
- Ei standardeja vielä, laiteyhteensopivuus pitää tarkastaa ennen hankintaa
- **POE** [Sivu 39] ei riitä suuriin järjestelmiin, lisäksi vaatii POE yhteensopivat kytkimet.
- Ulkokamerat: Ulkoinen verkkopiste saattaa olla turvallisuusriski. Tarvitsee vastaavanlaisen kokoonpanon kaapelointeineen kuin analoginen kamera.
- Kuvatahti riippuu enemmän olemassa olevasta kaistasta
- Kuvanopeudet alhaisemmat
- Kaikissa kameroissa ei ole automaattista valaistuksen säätöä

### 4.4.2 IP-kamerat

IP-kameroissa käytetään samoja tekniikoita kuin nykyaikaisissa digitaalikameroissa eli niissä on jo **CMOS-kennoja** [Sivu 39], joka on kehittyneempi kuin CCD-kenno. IP-kameroiden resoluutiosta puhuttaessa puhutaan yleensä Megapixeleistä, joka lyhennettän Mpix. Mitä suurempi Mpix luku on, sitä suurempi on kuva-ala, joka näkyy kuvassa, esim. 3 Mpix kamerassa on pikseleitä vaakatasossa 2048 ja korkeussuunnassa 1536. Viimeisimpien tutkimusten mukaan ihmisen tunnistukseen (kasvojen) ja ajoneuvojen rekisterikilpien tunnistukseen tarvitaan kuvaan noin 130 pikseliä / metri. Nykypäivän uusimmat IP-kamerat käyttävät uusinta kuvanpakkaustekniikkaa, joka on H.264-tekniikka. Tällä pakkaustekniikalla saadaan kuvakokoa pienennettyä kuvan laadun siitä kärsimättä. Esimerkiksi, jos JPEG kuva on 1, niin MPEG-4 kuva on 0,3 – 0,5 ja muunnos tästä H264, jolloin kuvan koko on 0,07 – 0,3. Pienennys kerroin on molemmissa tapauksissa 3 – 4 kertainen. Tällä saadaan aikaan se, että maksimi verkkokuormitus siirtoverkossa pienenee, jolloin voidaan kuvan kokoa suurentaa ja näin saada parempi laatuista kuvaa tallennettua.

### 4.4.3 Hybridikamerat

Hybridikamerat ovat IP-kameroita, joiden kuvan prosessointi tapahtuu IP-kameratekniikan tavoin, mutta kamera voidaan liittää suoraan sekä analogiseen tai TCP/IP-vekkoon ilman videopalvelinta. Hybridikamerat voivat lähettää kuvaa samanaikaisesti sekä analogiseen- että TCP/IP-verkkoon[6]. Em. kameran hyvänä puolena on se, että siirtyminen TCP/IP-tekniikkaan voidaan toteuttaa vaiheittain.

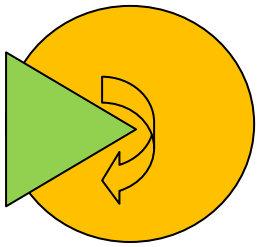
# 5. Kameravalvontajärjestelmään liitettävät ”älykkäät” anturit

Seuraavassa muutama yleisin kameravalvontajärjestelmään liitettävä komponentti, joilla saadaan lisää toiminnallista älykkyyttä kameravalvontajärjestelmiin.

## 5.1 Laser-skannerit


Laser-skannerit on alun perin kehitetty teollisuuden vaativiin konenäkösovellutuksiin, missä niitä on käytetty turvaratkaisuissa jo vuosikymmeniä. Ohjattaessa laser-skannereilla teollisuuden prosesseja, ovat valvontaetäisyydet yleensä vain muutamia metrejä[5].

Laser-skannereiden tekniikan kehittyminen erityisesti skannereissa käytettävien peilien hiontatekniikan parantuminen on mahdollistanut laser-skannereiden käytön yhä pitemmille etäisyyksille. Nykypäivän laitteilla voidaan luotettavasti toimia jopa 250 metrin etäisyyksille saakka. Laser-skannerin valvonta-alan kulma voi olla jopa 300°[5]. Edellä annettujen numeeristen arvojen perusteella saadaan valvotun sektorin pinta-ala. Sektorin pinta-ala lasketaan seuraavalla kaavalla:

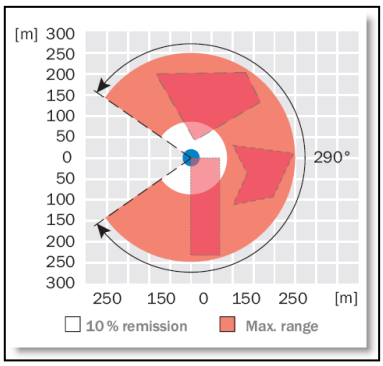


**Sektori A = α/360° * π r² => 300°/360° * π 250² = 163 624,60 m²**

Parhaimpien laser-skannereiden valvonta-ala on siis noin 165 000 m² eli 16,5 ha. Älykkäässä kameravalvontatekniikassa laser-skannereita voidaan hyödyntää sekä vaaka- että pysty- skannauksessa useammalla eri käyttötavalla. Yhdessä nykypäivän kehittyneen dome-kameratekniikan kanssa laser-skannereilla voidaan valvoa siis todella suuria alueita.

Laser-skanneritekniikan valvontajärjestelmien käyttäjiä löytyy sekä teollisuuden että viranomaistenkin joukosta. Runsaiden käyttösovellutusten johdosta on suuri joukko käyttäjäkuntaa, joille ko järjestelmä soveltuu useaan erilaiseen käyttöön.

### 5.1.1 Ominaisuudet

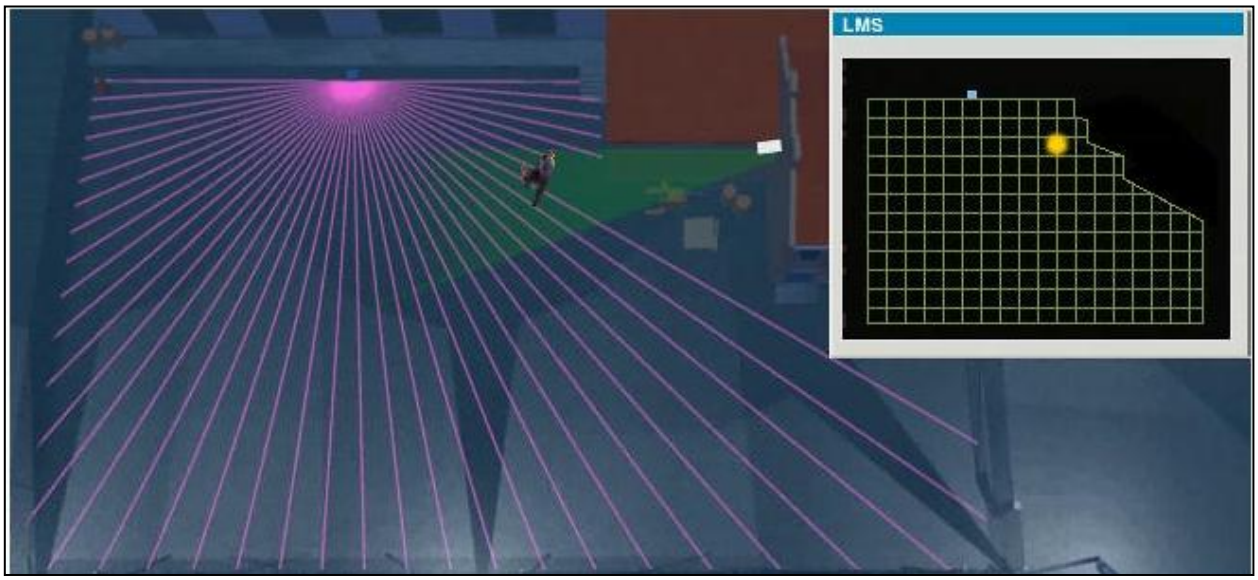



Laser-skannerin toiminta perustuu pyörivään peilitekniikkaan, jossa peilin pyörähdysaika on noin 13 ms eli alue skannataan noin 78 kertaa sekunnissa. Laser-skannereiden ominaisuudet riittävät erittäin haasteellisten kohteiden valvontaan. Laser-skannereissa on suuri joukko mitta- ja raja-arvoja, joita voidaan muuttaa valvottavan kohteen ominaisuuksien, koon ja valvontatason mukaan. Laser-skannereiden valvonta-alue voidaan rajata ohjelmallisesti halutulla tavalla. Näitä valvonta-aloja voidaan asettaa samaan kohteeseen useita, jotka voidaan kello-ohjatusti / kalenteriohjatusti asettaa päälle ja pois. Ulkopuoliset häiriötekijät kuten lintujen ja pieneläinten aiheuttamat häiriöt voidaan ohjelmallisesti estää valitsemalla kohteen koko ja nopeus oikein[5]. Käyttökohteita valittaessa pitää muistaa se, että lasersäteen eteen tulevat kohteet aiheuttavat valvonta-alueelle katveen.

### 5.1.2 Käyttösovellutukset

Laser-skannereiden käyttö kameravalvontajärjestelmän osana on antanut paljon laajemman aluevalvonnan valvonta-alan yhdessä kehittyneen kameratekniikan kanssa. Perinteisessä kameravalvontasovellutuksessa kamera on käännetty seuraamaan esim. toimialueen pääporttia, jolloin muualta, kuin portista tullut henkilö on jäänyt kameran valvonta-alueen ulkopuolelle. Laser-skannereiden käytön myötä kameravalvontajärjestelmästä on tullut jo ns. ”puoliautomaattinen” valvontajärjestelmä. Alueelle tunkeutumisen tapahduttua laser-skannerin lähettämän laservalon takaisin heijastumasta saadaan kulmatieto ja etäisyys, joka muunnetaan kameralle paikkatiedoksi, jonka perusteella kamera kääntyy asetettuun esiasentoon[5].

Digitaalitallennin tekniikan ja videovaihteiden hälytysyksiköiden ansiosta tämä toiminto saadaan ns. ponnahduskuvana hälytysmonitorille, josta valvomotyöntekijä ottaa tilanteen jatkokäsittelyyn manuaalisesti. Laser-skanneri ja domekameratekniikka mahdollistaa myös sen, että järjestelmä seuraa kohdetta automaattisesti. Seuraavalla sivulla olevassa kuvassa periaatteellinen kuva ko toiminnasta.




Laser-skannereiden käyttökohteina ovat suuret alueet missä vapaa liikkuminen on rajoitettu tai kielletty. Laitteilla voidaan valvoa piha-, varasto-, ja vesistöalueita. Muita käyttökohteita laser-skannereille löytyy mm. rakennusten kattojen ja seinien valvonnasta, satama-altaiden, lentokenttien ja jopa alusten suojaamiseen niiden ollessa satamassa. **Liitteessä 2** on muutamia laser-skannerin käyttösovellutuksia tarkemmin.

## 5.2 Muut tunnistimet, valaisimet ja järjestelmät

Älykkäässä kameravalvontajärjestelmässä voidaan käyttää runsaasti myös muita totutusta poikkeavia tunnistimia, valaisimia ja muita rikosilmoitinjärjestelmäntekniikkaan kuuluvia komponentteja. Seuraavassa muutamia yleisimpiä kameravalvontajärjestelmään liitettyjä komponentteja ja niiden mukana tuomia lisäominaisuuksia.

### 5.2.1 PIR-tunnistimet

Rikosilmoitinjärjestelmistä tutut PIR-tunnistimet (passiivinen infrapunatunnistin) voidaan liittää useisiin domekameratekniikalla toimiviin kameroihin. PIR-tunnistimen toimiessa saadaan kamera kääntymään haluttuun esiasentoon. Parhaimpien PIR-tunnistimien toimintaetäisyys on jo noin 150 – 180 metriä ja ne soveltuvat erinomaisesti ulkokäyttöön. Domekameroissa olevat hälytyssisäänmenot mahdollistavat muutamien esiasento-toimintojen toteuttamisen jo kameralla, kuin aikaisemmin se vaati erillisen järjestelmän ja sen myötä kahden järjestelmän integraation.

### 5.2.2 Näkyvä- /IR-valaistus

Valaisimia on jo pitkään käytetty aluevalvontakamerajärjestelmissä lisävalaistusta tuomassa. Valaisimina käytetään yleensä ajoneuvokäyttöön tarkoitettuja pistemäisiä lisäkaukovaloja, joilla pystytään valaisemaan jopa 500 – 750 metriin.

Joissakin kohteissa paljain silmin näkyvän valon määrää ei haluta lisätä, vaan tällöin kohteissa käytetään IR-valaisimia. IR-valaistuksen (Infrapunavalaistuksen) käyttö vaativissa kohteissa on yleistynyt. Tähän on ollut tietenkin syynä valaisimen tekniikan kehittyminen, käyttöiän pidentyminen ja hinnan laskeminen. Yksi tärkeä syy on myös CCTV-kameratekniikan kehittyminen, jolla IR-valaistuksessa voidaan nähdä lähes yhtä hyvin kuin päivällä. IR-valojen hintataso on noin 300 – 3 000 euroa ja tällä rahalla saadaan silmälle näkymätöntä valaistusta aina 30 – 1 000 metriin asti.

### 5.2.3 Rekisteritunnistusjärjestelmät

Kameratekniikan ja tietotekniikan kehittyminen on tuonut mahdolliseksi toteuttaa rekisterikilpien tunnistamisen ja siihen liittyvän kulunohjauksen. Järjestelmällä pystytään tunnistamaan useiden maiden rekisterikilvet ja niissä esiintyvät erilaiset kirjaimet, numerot ja merkit[3]. Tällä järjestelmällä pystytään antamaan kulkuoikeuksia niin jatkuvaan ajoneuvoliikenteeseen kuin myös yksittäistä ajotapahtumaa varten. Yksittäisen ajotapahtuman käyttö päättyy automaattisesti, kun ajoneuvo menee valvotulle alueelle ja tulee valvotulta alueelta pois. Tämä toiminto voidaan rajata myös aikaohjatusti tietylle aikavälille, milloin esim. kuljetuksen pitää olla kohteessa tai muutoin kulkuoikeus poistuu. Järjestelmään voidaan luoda erilaisia listoja, joille voidaan antaa eri toimintoja esim. kulkuoikeus jokaisena arkipäivänä työaikana tai ei-toivotuista rekisteritunnuksista hälytys. Tällaisten järjestelmien käyttökohteita löytyy runsaasti teollisuudesta, pysäköintitaloista ja jopa liikenteen seurantajärjestelmistä. Järjestelmästä saatava hyöty syntyy vasta sitten, kun toimipisteitä on runsaasti tai samassa toimipisteessä on ko ajoneuvolla runsaasti liikennöintiä alueelle ja sieltä pois.

# 6. Datansiirron TCP/IP verkkoratkaisut

## 6.1 TCP/IP-verkot

TCP/IP *(Transmission Control Protocol / Internet Protocol)* on usean Internet-liikennöinnissä käytettävän tietoverkkoprotokollan yhdistelmä. IP-protokolla on alemman tason protokolla, joka vastaa päätelaitteiden osoitteistamisesta ja pakettien reitittämisestä verkossa. Sen päällä voidaan ajaa useita muita verkko- tai kuljetuskerroksen protokollia, joista TCP-protokolla on yleisin. TCP-protokolla vastaa kahden päätelaitteen välisestä tiedonsiirtoyhteydestä, pakettien järjestämisestä ja hukkuneiden pakettien uudelleenlähetyksestä[10].

### 6.1.1 Ominaisuudet ja käyttökohteet

TCP/IP:n tärkein tehtävä on saada erilliset fyysiset verkot yhdistettyä ja toimimaan yhtenä kokonaisuutena. TCP/IP tarjoaa erilaisia palveluita, jotka perustuvat sen päällä toimivien protokollien ominaisuuksiin[10].

IP tarjoaa pakettikuljetuksen kaikille TCP/IP-protokollille. IP-verkon perussiirtoyksikkö on IP-tietosähke tai datagrammi. IP on yhteydetön ja kuittaamaton verkkopalvelu, joka ei varmista IP-pakettien perille pääsyä. IP määrittää vain kolme asiaa:

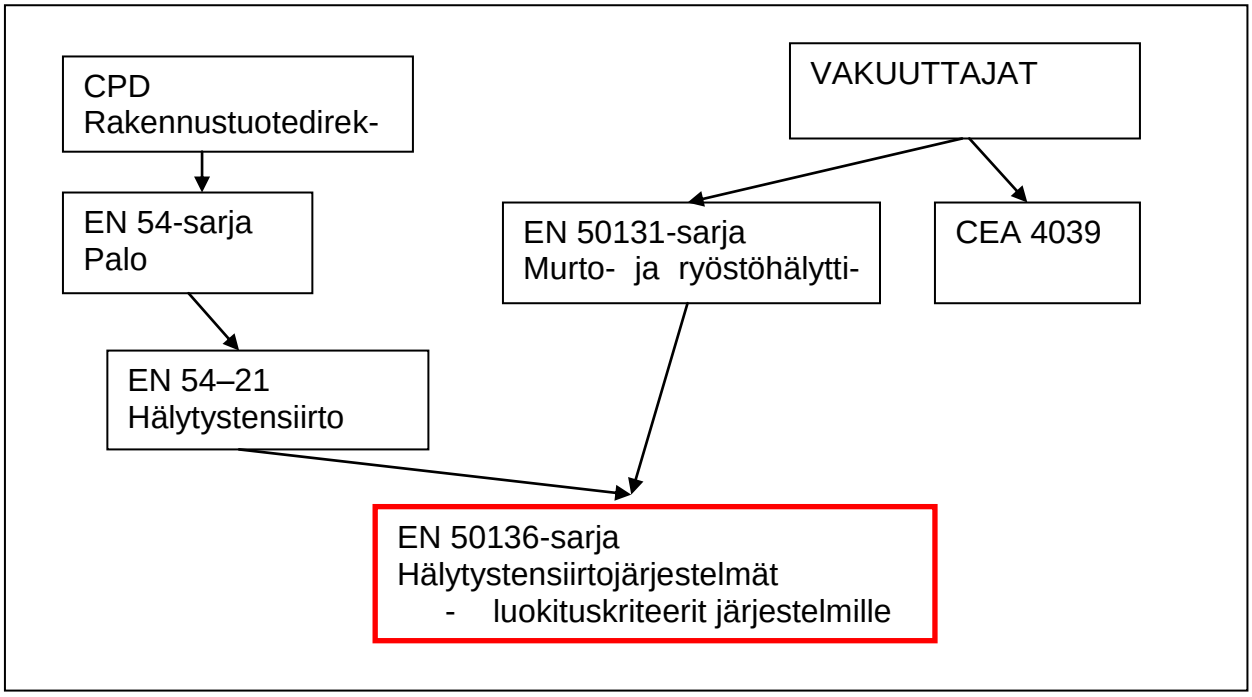
- TCP/IP-verkossa tapahtuvan kuljetuksen
- IP-ohjelmat valitsevat reitit, joita pitkin tiedot kuljetetaan
- IP sisältää joukon sääntöjä, joilla määritetään kuinka reitittimien tulee käsitellä paketit[10]

TCP on yhteydellinen ja luotettava protokolla. TCP vastaa viestien segmentoinnista, niiden uudelleen kokoamisesta, viestien uudelleen lähetyksistä ja segmenttien kokoamisesta kokonaisiksi viesteiksi ja virheen korjauksesta[10].

## 6.2 Kehittyneet TCP/IP-pohjaiset turvaverkkoratkaisut

Kehittyneiden TCP/IP-pohjaisten turvaverkkoratkaisujen vaatimukset ovat kehittyneet vuosien myötä kahdesta eri EU:n säädöskokonaisuudesta. Lähtökohtana ovat olleet CPD Rakennustuotedirektiivi ja Vakuutusyhtiöiden antamat säädökset vakuutuksista.

Seuraavassa kaaviossa on esitetty nykyisin voimassa oleva direktiivi ja sen miten se on muotoutunut. Direktiivi EN 50136 määrittää hälytyksensiirtojärjestelmän vaatimukset[2].

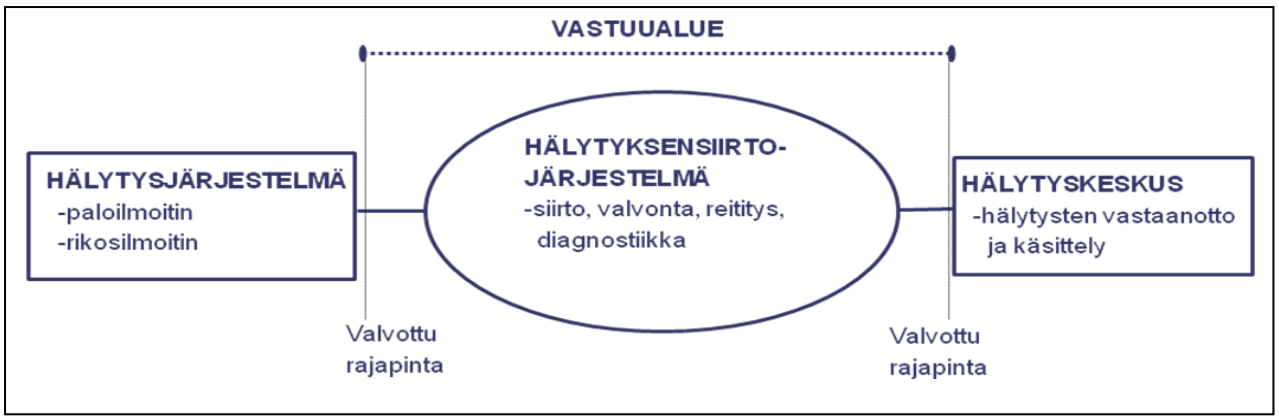



Esimerkiksi ISS Security Oy:n ipHSJ-hälytyksensiirtopalvelu on tarkoitettu erityisen vaativien tiedonsiirtotarpeiden, kuten automaattisten paloilmoitinjärjestelmien ja kriittisten kohteiden hälytysjärjestelmien tuottamien hälytysten siirtoon hätäkeskuksiin ja vartiointiliikkeisiin. Palvelu täyttää viranomaisten ja vakuutusyhtiöiden hälytyksensiirrolle asettamat korkeimman luokan (luokka 4) vaatimukset[2].

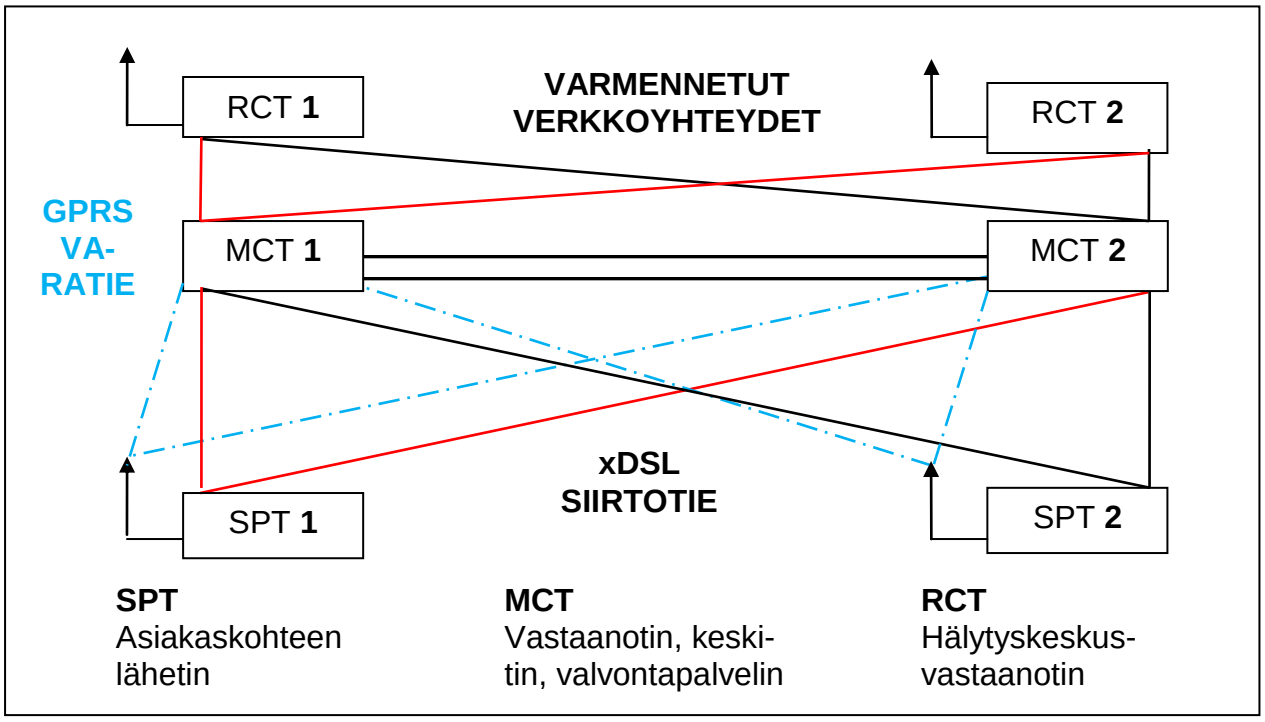
Tämä hälytyksensiirtojärjestelmä on luokituslaitoksen tarkastama ja se täyttää EN 50136-1-1 palo- ja rikosilmoitinjärjestelmien tiedonsiirtoa koskevan standardin mukaisten luokkien D4, M4, T5, A4, S2 ja I3 vaatimukset. Alla olevassa taulukossa on mainittuihin luokkiin liittyviä arvoja.

| | | |
|---|---|---|
| D4 | Siirtoaika avg < 10s | 95 % < 15s |
| M4 | Maksimisiirtoaika | 20s |
| T5 | Raportointiaika | 90s |
| A4 | Saatavuus | 99,8 % / vuosi |
| S2 | Korvauksenesto | korkein |
| I3 | Tietoturva | korkein |

Hälytyksen siirron kokonaisuudesta ISS Security Oy:n ISS Turvaverkko® käsittää seuraavalla sivulla olevan kuvan mukaisesti lähettimen ja vastaanottimen väliin jäävän tekniikan.




Periaatteena on se, että kaikki hälytyksensiirtojärjestelmän laitteet on kahdennettu asiakaskohteesta hälytyskeskukseen. Varsinainen siirtoverkko toteutetaan aina kahden eri operaattorin yhteyksillä. Kiinteät siirtotiet varmistetaan vielä kahdella erillisellä GPRS-yhteydellä[2]. Alla olevassa kuvassa hälytyksensiirtojärjestelmä tarkemmin periaatekuvana.




### 6.2.1 Ominaisuudet ja käyttökohteet

ISS Turvaverkko® järjestelmään voidaan liittää kaikki viranomaisten hyväksymät automaattiset palo- ja rikosilmoittimet ja se soveltuu erityisesti kohteisiin, joissa edellytetään korkeinta mahdollista valvonnan tasoa. ISS Turvaverkko® järjestelmää voidaan käyttää videokuvan siirtämiseen valvontakohteesta keskitettyyn valvomoon. Palveluun liittyvät muut ominaisuudet ovat seuraavat; järjestelmä on kaksisuuntainen, digitaalinen ja siinä

on kaksi erillistä fyysistä tietoliikennerajapintaa eli useita siirtoteitä. Yhteyksien yli voidaan siirtää mitä tahansa dataa ja näin se sallii useiden palvelujen vaatimat yhteydet. Yhteys on päästä päähän valvottu ja tapahtumien seuranta tallentuu. Verkonvalvonta on yksi tärkeä osa hälytyksensiirtoverkkoa, koska direktiivin EN 50136-1-1 vaatimus on saatavuuden osalta 99,8 % /vuosi. Tämä aiheuttaa sen, että pienetkin viat on huomattava ja niihin on voitava puuttua ennen, kuin ne aiheuttavat merkittäviä ongelmia.

Etuna perinteisiin ratkaisuihin verrattuna on se, että tarvitaan ainoastaan yksi tietoliikenneyhteys kiinteistöä kohti useiden palvelujen tuottamisen. Päätelaite pystyy valvomaan samaan verkkoon kytkettyjen laitteiden toimintaa. Ominaisuuksia voidaan lisätä; esim. perinteinen modeemiyhteydellä varustettu rikosilmoitinkeskus voidaan lisäkortin avulla ”nostaa IP:n päälle” [2].

Salaus on toteutettu AES (Advanced Encryption Standard) 128 bit salauksella. Tähän liittyvät väärennöksen (korvauksen) esto, yksilöllinen laitetunniste, sanoman toiston esto (sanoman kaappauksen ja uudelleen lähetyksen esto) ja tunnistus 128 bit koodin ja sarjanumeron yhdistelmällä. Kaikki sanomat on sarjanumeroitu väärennöksen estämiseksi.

Varmuutta saadaan lisää myös varmentamalla järjestelmän sähkönsyöttö vikatapausten varalle niin akustoilla kuin dieselgeneraattoreillakin.

## 7. Tallennintekniikka

Nykypäiväisen kameravalvontajärjestelmän tärkeimpiä komponentteja on kuvantallennustekniikka. Kuten kaikilla kameratekniikan osa-alueilla, niin myös digitaalitallennintekniikassa on tapahtunut paljon kehitystä lyhyessä ajassa. Ensimmäiset digitaalitallenninjärjestelmät otettiin käyttöön 1990-luvun loppupuolella. Tällöin kiintolevyjen koot olivat vain murto-osa tämän päivän kokoluokista. Kuvanpakkausformaatti oli pelkästään JPEG-muotoa, kuvakoko QCIF tai CIF ja yksittäisen kuvan koko oli noin 10 - 15 kbit. Tallennetun kuvan määrä maksimissaan noin 4 kuvaa/s ja tallennusajat olivat vain muutamia vuorokausia.

Tilanne tänä päivänä on se, että digitaalitallentimet pystyvät tallentamaan reaaliaikaista kuvaa jokaiselta liitetyltä kameralta ja tallennusajat ovat jopa useita kuukausia. Kuvan-

pakkausformaatit (MPEG-4 / H264) ovat kehittyneet entistä paremmaksi, jolloin yhden kuvan koko on vain noin 1,5 kbit. Kuvakoon pieneneminen mahdollistaa etäkuvavalvomoiden käytön entistä joustavammin. Digitaalitallentimilla voidaan tallentaa yhdeltä kanavalta jopa satoja kuvia sekunnissa, jolloin nopeidenkin prosessien vaiheiden tallentaminen ja tarkastelu on mahdollista ja prosessivirheiden korjaaminen on tullut mahdolliseksi. Tällaisten ominaisuuksien ansiosta prosessiteollisuudessa on saavutettu tuotantolinjoilla yhä parempia tuotantonopeuksia.

Digitaalitallentimien kiintolevykapasiteetin kasvaminen jopa useisiin teratavuihin mahdollistaa kuvamateriaalin tallentamisen pitkäksi aikaa. Digitaalitallentimen sisään voidaan rakentaa tänä päivänä noin 3 – 5 Tb:n kiintolevykapasiteetti ja ulkopuolisilla jäähdytetyillä kiintolevypakoilla päästään useiden kymmenien teratavujen tallennustilaan. Lisäksi digitaalitallentimessa saattaa olla jopa kahdeksan erillistä kiintolevyä RAID5 järjestelmässä. Tällä pyritään pienentämään tiedon menetyksen riskiä, jos kovalevyistä jokin rikkoutuu syystä tai toisesta. Tämäkään ei välttämättä yksistään riitä huippunykyaikaisten koneiden ja korvaamattomien tietojen kohdalla, vaan tallentimen tiedot varmistetaan tarvittaessa muille erillisille kiintolevypakoille.

Paremmat digitaalitallentimet on itsessään varmennettu vikasietoisilla virtalähteillä ja usealla tuulettimella koneen jäähdyttämiseksi. Koneiden toiminnan varmentaminen ei yksistään riitä, vaan koneiden sijaintipaikka eli laitetilat on oltava asianmukaisesti rakennettuja. Tallennin ja muut verkkolaitteet on sijoitettava hyvin ilmastoituun tilaan, jonka lämpötila on jatkuvasti valvottu. Lämpötila on säädetty 20° - 25 °C asteeseen, jotta komponenteilla olisi optimaalinen käyttöikä, eikä mahdollisia ylikuumenemisia tapahdu.

## 7.1 Paikalliset kuvantallennustekniikat ja niiden käyttösovellutukset

Digitaalitallennusta käytetään lähes poikkeuksetta paikallisena sovellutuksena. Tähän on varmaan useita syitä, mutta esim. teollisuuden parissa toimintojen keskittäminen on vasta nyt alkamassa nykyisen laskusuhdanteen myötä. Paikallisissa tallenninsovellutuksissa ns. etähallintaa on käytetty vain paikallisesti tapahtuneiden asioiden tutkinnassa ns. asiakas-ohjelmistolla.

Tallentimissa voidaan käyttää sekä analogisia että IP-kameroita. Paikallisissa tallennustekniikoissa on etuna se, että kuvat tallentuvat aina, kunhan järjestelmän sähkönsyöttö

on kunnossa. Digitaalitallentimen ohjelmapäivitykset ovat suhteellisen vähäisiä. Pieniä ohjelmistopäivityksiä tulee muutaman kerran vuodessa. Digitaalitallentimet kannattaa päivittää esim. kerran vuodessa jolloin digitaalitallentimen tallennustekniikka toimii moitteettomasti tallentimen elinkaaren ajan. Päivitysten yhteydessä on tärkeä myös huolehtia, että digitaalitallentimet puhdistetaan sisältä ja tuulettimien suodattimet vaihdetaan uusiin.

Paikallisessa tallennuksessa on runsaasti etuja, mutta myös joitakin haittoja. Seuraavassa ko. järjestelmään liittyvät ominaisuudet:

Paikallisen tallennuksen hyvät puolet[8]:

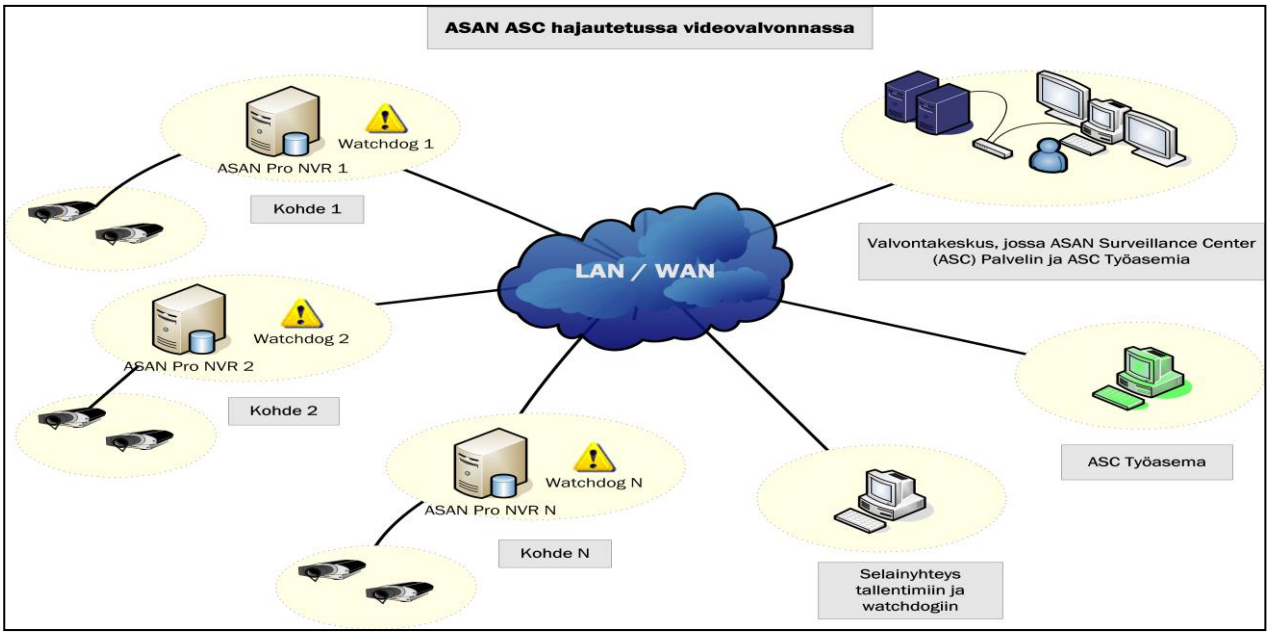
- Digitaalitallennin kohteessa mahdollistaa paikallisen valvonnan pienemmillä toimenpiteillä, joista ei varsinaisia käyttökuluja synny
- Siirtoverkon (Sonera / ELISA / muut fyysisen verkon omistajat) katkot eivät vaikuta tallentamiseen
- Sisäverkon (LAN) kaista edullista
- Tallenteet paikallisesti saatavissa tarvittaessa pikaisesti käyttöön
- Etävalvonta mahdollista myös LAN verkon alueella

Paikallisen tallennuksen huonot puolet[8]:

- Yleensä ei varmennuksia (RAID, Backup)
- Digitaalitallentimen rikkoutuminen mahdollisesti hävittää tallenteet
- Vikasietoisuus ja hankintakustannukset kalliimpi
- Korjauskustannukset korkeammat
- Tietoturva käyttäjän harkinnassa

Mikäli paikallisissa kohteissa käytetään runsaasti IP-kameroita ja korkeita kuvatahteja tallennuksessa. Seuraavassa on esimerkkilaskelma siirtokapasiteetin vaikutuksesta siirtoaikaan. Paikallisessa tallennusjärjestelmässä, joka käytetään omaa verkkoa ja jonka kapasiteetti on 1 Gbit/s. Tallennetaan materiaali korkealla kuvatahdilla 10 kuvaa/s ja käytetään esim. 1,3 Mpix IP-kameroita. Jouduttaessa tilanteeseen, että etävalvomosta pitää katsoa kuvatallenteita esim. 1 Mbit/s siirtotietä käyttäen. Tällöin yhden minuutin pituisen tallenteen siirtäminen kestään noin 4 – 8 minuuttia. Mikäli käytettäisiin esim. analogisia kameroita ja kuvan koko on 4 CIF, on tällöin yhden minuutin pituisen tallenteen kuvansiirtoaika vain noin 1,5 – 2,5 minuuttia[1]. Seuraavalla sivulla olevassa kuvas-

sa on esimerkki keskitetystä valvomoratkaisusta, mikä koostuu useista paikallisista kuvantallennusjärjestelmistä[3].

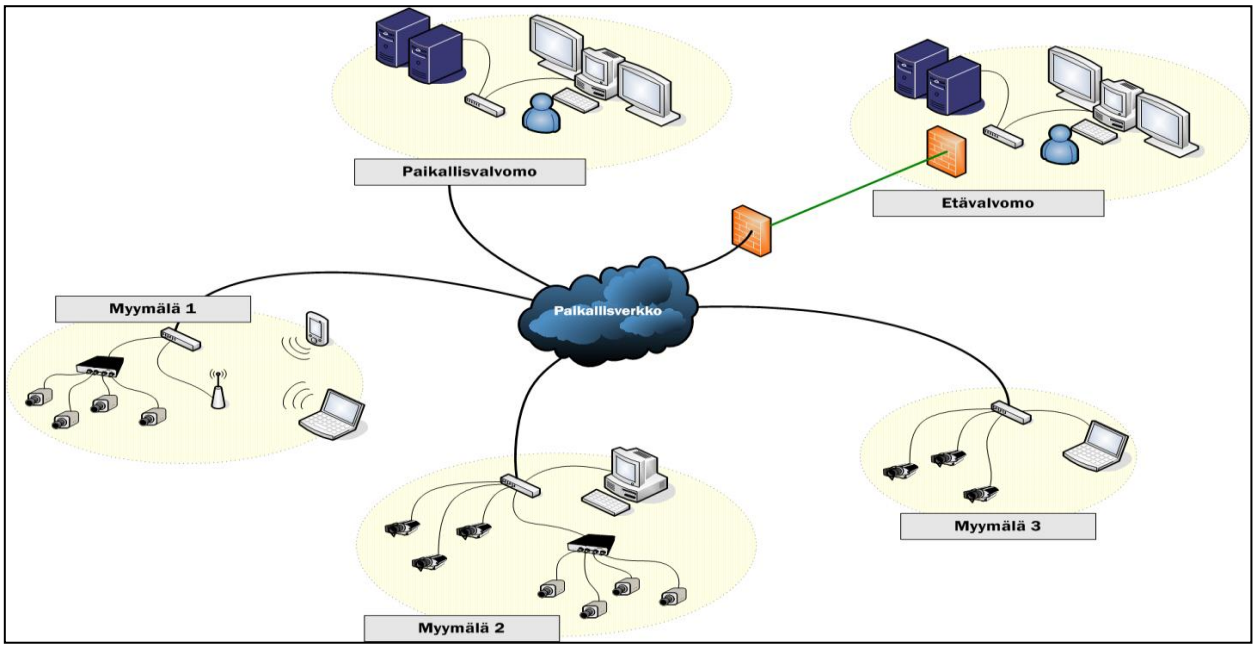



## 7.2 Keskitetty kuvantallennustekniikka ja sen käyttösovellutukset

Yleistyvän IP-kameratekniikan myötä on Suomessa useassa yrityksessä toimipisteiden kuvatallenteet keskitetty yhteen keskitettyyn tallennusserveriin. Tiedonsiirtoverkkojen kapasiteetin kasvu ja hintatason lasku on mahdollistanut tällaisen tekniikan käyttöönoton. Yritysten omien TCP/IP-verkkojen kapasiteetit ovat jo 100 Mbit/s – 1 Gbit/s suuruusluokkaa, joten keskitettykuvantallennus onnistuu.

Keskitetyssä tallennustekniikassa on hyvänä puolena tallentimen hankintahinta ja kappalemäärät, mutta tallennuskapasiteetin määrittäminen on vaikeampi ratkaista. Keskitetyn tallennustekniikan ongelma on IP-kameratekniikan tuottama jatkuva verkkokuorma varsinkin, jos samassa verkossa pitäisi toimia yrityksen toimisto- tai tuotantoverkko. Toimisto- ja tuotantoverkkoon liitetyn turvallisuusjärjestelmän huolto ja päivityksiin tarvittavaa tieto taitoa ei välttämättä ole yrityksen IT-osastolla. Ongelmia tulee IP-kameratekniikan kuvien tallennuksen kanssa, koska huolto- ja päivitysajot toteutetaan yleensä iltaisin ja viikonloppuisin, jolloin kameratekniikan pitäisi olla ehdottomasti valvontakäytössä. Keskitetyn tallennustekniikan suurin ongelma on se, että kuvia ei voida tallentaa, jos yhteys etäkohteeseen katkeaa.

Alla olevassa kuvassa on periaatekuva keskitetystä etävalvomosta, jossa suoritetaan etäkohteiden kamerakuvien tallentaminen[3].




**Liitteessä 3** on kaksi erillistä laskentaesimerkkiä verkon maksimikuormasta käytettäessä kahta erilaisella kuvakoolla varustettua kameraa.

Etätallennuksen hyvät puolet[8]:

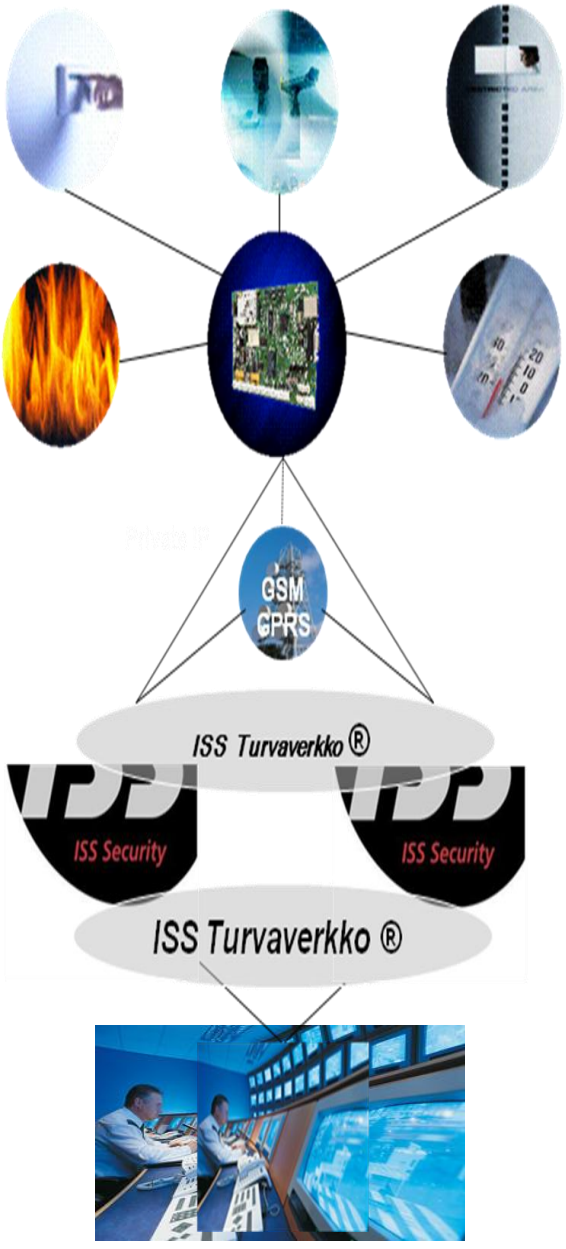
- Mahdollistaa pienemmät käyttökustannukset
- Tallennin valvotussa tilassa, jossa keskitetty tallenteiden käsittely
- Varmennettu data, vikasietoisuus tallentimien osalta hyvä
- Palvelumaksut, jolloin ei suuria kertainvestointeja
- Ei korjauskuluja, palvelusopimuksesta riippuen
- Pienempi laitemäärä kohteessa, ainoastaan kamerat ja verkkoyhteys

Etätallennuksen huonot puolet[8]:

- Siirtoverkon katkot estävät tallennuksen ja etäkohteiden kuvien katselun
- Vaatii kaistaa siirtoverkolta
- Kuvatahdit pienemmät, riippuen kaistan leveydestä ja halutusta kuvan laadusta
- Kuvan laatu saattaa olla heikompi, riippuen kaistan leveydestä ja kuvatahdeista
- Palvelumaksut

## 8. Valvomotekniikka uudessa TCP/IP-pohjaisessa turvaverkossa

Valvomotekniikoiden kehittyessä ei voida suoraan sanoa mikä on paras toteutusratkaisu kuhunkin tapaukseen. Valvomotoiminnan keskittämistä suunniteltaessa kannattaa kääntyä alan asiantuntijoiden puoleen, sillä hankkeeseen liittyy paljon suuria kokonaisuuksia, eikä tietoa niiden hallitsemiseksi välttämättä ole oman yrityksen henkilöstöllä. Tiedonsiirtoverkon, servereiden (mitoitus, sijoitus, päivitykset), tietoturvan, Client-koneiden ja valvomo-ohjelmistojen valinnassa on paljon tuotteita ja yksityiskohtia, jotka edellyttävät omaa ammattitaitoa, kuten määrittelyt, verkon kapasiteetti, millä kameratekniikalla, miten tallennus, mikä valvomo-ohjelmisto tukee valittuja tallentimia / kameroja jne. Seuraavassa kuvassa sellaisen nykyaikaisen TCP/IP-pohjaisen turvaverkon ominaisuuksia, joilla voidaan siirtää tarvittavaa datatietoa turvallisesti kohteesta valvomoon.




**Valvottavat kiinteistöt**
- integroitu sanomanvälitys uusille järjestelmille
- kahdennettu siirtotie – IP ja GPRS
- valvotut yhteydet
- salattu lähetys
- verkkohyökkäysten tunnistus 180 sekunnin sisällä

**Verkkohyökkäyksen tunnistus**
- hälytinlaite ja LAN toimimattomuus 90 sekuntia
- IP verkon valvonta joka 30 sekunti
- paikallinen GSM tarkistus joka 10 sekunti
- GPRS verkon tarkistus …
  - IP kunnossa joka 30 minuutti
  - IP epäkunnossa joka 3 minuutti

**Siirtotietarkistus**
- jatkuva siirtoteiden ja vastaanottolaitteiden pollaus niiden toimintakunnon tarkistamiseksi

**ISS Palvelukeskus**
- kahdennettu
- turvallinen, skaalautuva vastaanottoteknologia
- redultanttinen tekniikka

**Hälytysten vastaanotto**
- turvallinen, skaalautuva vastaanottoteknologia
- monistetut hälytysten siirtoyhteydet
- turvallinen, valvottu ja salattu lähetystekniikka

## 8.1 Suunnittelu ja turvallisuus

Turvallisuusvalvomotoimintaa keskitettäessä kaiken suunnittelun lähtökohtana on oltava asiakkaan toiminta ja asiakkaan liiketoimintaan liittyvät riskit. Turvallisuusvalvomotoiminnan keskittämistä suunniteltaessa on jo hyvissä ajoin tehtävä tarvittavat palveluntuottajan ja – toteuttajan kilpailutukset, jolloin aikaisessa vaiheessa päästään keskustelemaan alan ammattilaisten kanssa tarvittavista yksityiskohdista, sillä valmista kokonaisuutta harvoin löytyy sellaisenaan. Riittävän ajoissa suoritetulla avoimella kumppanuushenkisellä keskustelulla, hyvällä yhteistyöllä ja suunnittelulla valitun palveluntuottajan ja -toteuttajan kanssa, saadaan valitusta tekniikasta huomattavasti enemmän kustannussäästöjä ja käytettävyyttä.

Yrityksen on suunnitellessaan valvomotoiminnan keskittämistä jo suunnitteluvaiheessa kartoitettava valvomotoimintaa uhkaavat riskit ja niiden toteutuessa liiketoiminnalle aiheutuvat seuraukset. Huolellisesti suunnitelluilla ja toteutetuilla teknisillä ja toiminnallisilla järjestelyillä voidaan valvomon toimintaa uhkaavien riskien todennäköisyyttä ja vaikuttavuutta merkittävästi pienentää. Tässä vaiheessa tehty poikkeustilanteiden suunnitelmat on helpointa ja edullisinta toteuttaa. Poikkeustilannesuunnitelmaan on hyvä sisällyttää myös elpymissuunnitelma, joka valvomotoiminnassa on erittäin merkityksellinen kustannus mielessä.

Keskitetyn valvomon turvallisuustaso on sidoksissa suojattavaan liiketoimintaan. Useissa teollisuuden kohteissa vartioinnista vastaavat henkilöt toimivat myös esim. teollisuuspalokunnassa ja ovat näin ensiarvoisen tärkeässä roolissa ensivastetoiminnassa. Näissä tapauksissa etävalvomon toiminta ja olemassa olo korostuu ja saa suuremman roolin poikkeusolojen ajaksi. Useissa tapauksissa valvomotoiminnan merkitys liiketoiminnalle on niin keskeinen, että tavoiteltava turvallisuustaso ja hyväksyttävät riskit on käsiteltävä turvallisuusjohdon lisäksi yrityksen korkeimmassa johdossa. Valvomotoiminnan turvaamisessa on kiinnitettävä huomiota valvomon rakenteelliseen suojaukseen ja paloturvallisuuteen. Sähköä tarvitsevien kriittisten laitteiden (tietoliikenteen modeemi, reititin ja hubi, puhelinvaihde, valvomotyöasemat, kamerat, digitaalitallentimet jne.) toiminta on varmistettava myös sähkökatkojen ajaksi. Varavirtajärjestelyt on toteutettava siten, että valvomon toiminta kriittisten toimintojen osalta jatkuu riittävällä tasolla useita tunteja kestävien sähkökatkojenkin aikana. Laitetilojen ja valvomotilan ilmanvaihto- ja jäähdytysjärjestelmät on myös mitoitettava riittävän suuriksi, sillä laitteet tuottavat erit-

täin runsaasti lämpöä. Valvomotoiminnassa tietoturvallisuuteen (palomuurit, virustorjunta, varmuuskopiointi ja varajärjestelmät) on myös kiinnitettävä erityistä huomiota.

Kaikesta ennakkovarautumisesta huolimatta on todennäköistä, että jäljelle jää riskejä (tulipalo, vesivahinko, ylijännite sähköverkossa jne.) mitkä toteutuessaan voivat merkittävästi haitata tai jopa keskeyttää valvomon toiminnan useiksi päiviksi. Tällaisten vakavien vahinkotilanteiden varalle on tehtävä suunnitelma järjestelyistä, joilla pystytään turvaamaan toiminnan jatkuminen riittävällä tasolla.

## 8.2 Miksi keskitetty valvomotoiminto?

Yhteiskunnan arvojen muuttuminen ja siitä seuraava kilpailun koveneminen markkinaosuuksista pakottavat tekemään kustannustason leikkaamiseksi keskitettyjä palveluratkaisuja, joista yksi on keskitetty valvomotoiminta. Valvomotoiminnassa, joissa työskennellään 24/7, henkilöstön palkkakustannukset näyttelevät hyvin merkittävää osaa paikallisen valvomon kokonaiskustannuksissa. Tekniikan voimakkaan kehityksen ansiosta on valvomotoiminnan keskittäminen tullut yhä helpommaksi ja edullisemmaksi toteuttaa. Kehittyneen kamera- ja valvomotekniikan sekä tiedonsiirtoyhteyksien hinnat ovat laskeneet, joten keskitettäessä valvomotoimintoja, etävalvontatekniikan kustannukset pysyvät hyvin kohtuullisina. Hyvin usein keskitettäessä valvomotoimintoja tullaan toimeen merkittävästi pienemmällä vartijoiden kokonaismäärällä tai tehdyillä kokonaistyötuntimäärällä kuin hajautetussa ratkaisussa, joten palkkakustannuksissa voidaan saavuttaa merkittäviä säästöjä. Hälytysten vastaanottoon ja niiden edelleenvälittämiseen liittyvät palvelut eivät ole paikkakuntasidonnaisia, joten niidenkin keskittäminen on helppo toteuttaa palvelun laadun siitä muuttumatta tai kärsimättä.

Vaikeimmin järjestettäviä asioita ovat ne valvomon sijaintikohteelle antamat muut palvelut, mitkä edellyttävät henkilön läsnäoloa. Osa näistäkin palveluista voidaan tuottaa etäpalveluna tekniikan avulla, mutta osa tehtävistä jää kohteessa suoritettavaksi, ja ne yleensä edellyttävät paikallisia työjärjestelyitä. Mikäli kohteessa on välttämätöntä järjestää aulapalvelut, on useissa tapauksissa tarkoituksenmukaista liittää siihen kohteen turvallisuusvalvonta (paikallisvalvomo) kohteen aukioloaikana. Virka-ajan ulkopuolella kohteen valvonnassa voitaisiin tukeutua keskitetyn valvomon valvomopalveluihin ja tapauskohtaisesti paikalle hälytettävään vartijaan taikka muuhun alueella jo työskentelevään henkilöön, ellei toiminta vaadi vartijanoikeuksia.

Tietoliikenneyhteyksien siirtonopeuksien kasvu ja videokuvan käsittelyn kehittyminen mahdollistavat videokuvan siirtämisen keskitettyyn valvomoon tehokkaasti. Useissa tapauksissa videokuvan ja muun valvontainformaation siirtämiseen kannattaa varata oma verkko, koska yleensä toimistoverkon huolto ja päivitykset toteutetaan toimistoajan ulkopuolella iltaisin ja viikonloppuisin eikä verkko silloin ole käytössä. Valvonnan kuvansiirtotarve ja muun hälytysinformaation siirtäminen ajoittuu yleensä työskentelyajan ulkopuolelle. Käytettävissä oleva tekniikka antaa mahdollisuuden siirtää kuvaa esim. työskentelyaikana paikallisvalvomoon ja muuna aikana etävalvomoon.

Käytössä olevat palo- ja rikosilmoitusjärjestelmät ovat pääasiassa ns. osoitteellisia järjestelmiä, joista hälytystieto saadaan ilmaisinkohtaisesti. Useissa tapauksissa keskuksen antama osoitteellinen hälytystieto voidaan sellaisenaan siirtää etävalvomon valvomotyöasemalle. Haluttaessa voidaan esim. tilavalvontahälytykset ohjata eri valvomoon kuin palo- ja ryöstöhälytykset. Verkon välityksellä voidaan suorittaa myös esim. palo- ja rikosilmoituskeskuksen silmukoiden ohituksia sopivilla ohjelmistoilla.

Keskitetyssä valvomoratkaisussa vartijoiden ohjeistuksen tulee olla hyvin yksityiskohtaista, koska useissa tapauksissa vartijalla ei ole kohteen paikallistuntemusta tai se on hyvin vähäistä. Tähän on ratkaisuna laajat valvomo-ohjelmistot, joihin saadaan erilliset karttapohjat, mihin on sijoitettu kameraikonit, kameroiden valvonta-alat, portit jne. Keskitetyssä valvomoratkaisussa valvomon luotettavan ja häiriöttömän toiminnan merkitys kasvaa hajautettuun valvomoon verrattuna. Mahdolliset häiriöt ja keskeytykset keskitetyn valvomon toiminnassa saattavat vaarantavat laajemmin liiketoiminnan turvallisuutta, ja useissa tapauksissa myös käytännön toimintaa, kuin hajautetussa ratkaisussa.

### 8.2.1 Keskittämisellä saavutettavat kustannussäästöt

Valvomotoimintojen keskittämisellä saavutetaan huomattavia kustannussäästöjä, jotka saadaan aikaan, kun etävalvontakohteiden työaikoja voidaan pienentää. Seuraavassa esimerkinomaisesti esitettynä mahdollisesti saavutettavat kustannussäästöt palkkakustannusten osalta[4]. Toimintoja ei ulkoisteta ulkopuoliselle palveluntarjoajalle. Esimerkki seuraava:

- yrityksellä on viisi toimipistettä, jokaisessa on 24/7 vartiointipalvelu
- jokaisessa kohteessa on kaksi vartijaa ympärivuorokauden
- toiminnan toteuttamiseen tarvitaan yhteensä 45 henkilöä (9 hlö / kohde)

- palkkakulut sivukuluineen / henkilö, 4 000,00 €
- kustannukset toiminnasta kuukaudessa 180 000,00 €

Toimintoja muutetaan ja keskitetään seuraavasti:

- neljän toimipisteen kohdalla siirrytään 16/5 vartiointipalveluun, koska yövuorot ja viikonloput suoritetaan etäpalveluna viidennestä toimipisteestä
- em. toiminnan toteuttamiseen tarvitaan neljällä toimipisteellä yhteensä 20 henkilöä (5 hlö / kohde)
- etävalvomo toimipisteen toiminnan toteuttamiseen tarvitaan 12 henkilöä, koska yövuoroon lisättiin yksi henkilö suorittamaan etävalvontaa, yhteensä henkilöitä tarvitaan siis kaikkien toimipisteiden toiminnan toteuttamiseen 32 kappaletta.
- palkkakulut sivukuluineen / henkilö, 4 000,00 €
- kustannukset toiminnasta kuukaudessa 128 000,00 €
- **saavutettava kustannussäästö kuukaudessa on 52 000,00 € eli 28,9 %**

Em. laskelmassa ei ole otettu huomioon paikallisten valvomoiden toiminnan supistamisesta aiheutuvia ylimääräisiä ulkopuolisten vartioliikkeiden suorittamia hälytysajoja kohteisiin eikä etävalvomotoiminnan rakentamisesta aiheutuneita tiedonsiirtoverkon ja turvatekniikan laitekustannuksia. Kuten em. laskelmasta huomataan, ovat keskittämisellä saavutettavat kustannussäästöt kuitenkin varsin huomattavia.

## 8.3 Valvomotekniikka

Keskitetyn valvomon tekniikka pitää olla varmennettua, jotta mahdolliset laiteviat, tiedonsiirtoverkon ja sähkökatkon aiheuttamat ongelmat eivät lamauta keskitetyn valvomontoimintaa välittömästi. Keskitetyn valvomon tekniikka pitää olla yhdenmukaista kaikissa etäkohteissa, jotta valvomotyön tekeminen ei ole eri kohteiden välillä erilaista. Tästä saattaa seurata jonkin kohteen toimintojen seuraamisen vähentyminen ja siitä aiheutuvat palvelun laadun huononeminen.

### 8.3.1 Valvomotekniikka paikallisissa nykyaikaisissa valvomoissa

Paikallisvalvomossa, joka on osa keskitettyä erävalvomotoimintaa kameravalvontajärjestelmän tekniikka voi olla seuraavanlaista.

**Monitorien** pitää olla riittävän suuria, jotta niiden kuvaruutu voidaan jakaa nelikuvajakajilla neljäksi, sillä on paljon kohteita, joissa esim. portteja halutaan valvoa koko ajan ja lisäksi porttien kuvat tallentuvat yleensä suuremmalla kuvatahdilla. Monitorien koko riippuu katseluetäisyydestä, mutta koko vaihtelee yleensä 19” – 32” välillä. Monitorien määrä on riippuvainen valvottavien kohteiden määrästä ja kohteen kameroiden määrästä. Lähtökohtana voidaan pitää pienissä valvomoissa, että neljää kameraa kohden pitää olla yksi monitori.

**Operatiivinen toiminta** tapahtuu paikallisesti isoissa valvontakohteissa videovaihteen avulla. Paikallisten kohteiden etävalvontakohteet liitetään valvomoon ns. videovaihteiden välisenä satelliittiyhteytenä joko kuitu-, kupari- tai TCP/IP-pohjaisen turvaverkon kautta. Tällöin on mahdollista ohjata etäkohteen kameroita niin kuin ne olisivat ”kiinni” paikallisessa videovaihteessa. Tällä toiminnalla varmistetaan se, että valvontahenkilöstö osaa käyttää kaikkien kohteiden järjestelmiä yhtä hyvin. Lähtökohtana voidaan pitää, että jokaisesta valvontakohteesta pitää voida ottaa kaksi – neljä yhdenaikaista kuvaa keskitettyyn valvomoon. Pienemmissä valvontakohteissa voidaan käyttää valvontaohjelmistoja (esim. RMC tai Asan ASC), joiden kautta voidaan digitaalitallennin-pohjaista kuvan siirtää keskitetyn valvomon näytölle.

**Kuvamateriaalin tallennus** tapahtuu hajautetusti jokaisessa valvontakohteessa. Kuvamateriaalin tallennukseen valitaan sopiva digitaalitallennin käyttötarpeen mukaan. Digitaalitallennin voi olla joko analogia-, hybridi- tai IP-tallennin. Tallennettaessa kuvaa on hyvä muistaa kuinka kauan kuvamateriaalia halutaan säilyttää ja kuinka monta kuvaa sekunnissa miltäkin kameralta kuvaa tallennetaan. Näiden kokonaisuuksien kautta saadaan selville tarvittava kiintolevykapasiteetti. Periaate tallentimen valinnassa on se, että ”kaikkia munia ei kannata sijoittaa yhteen koriin” eli mieluimmin jaetaan kuvat vaikka kahdelle erilliselle tallentimelle kuin pelkästään yhdelle isolle tallentimelle.

**Digitaalitallennin** on isoissa valvontakohteissa vain tallennetun kuvahistoriatiedon säilyttämistä varten. Kuvamateriaali voidaan etävalvomosta käsin tarvittaessa käydä läpi.

### 8.3.2 Valvomotekniikka keskitetyssä etävalvomossa

Keskitetyssä etävalvomossa pitää olla riittävät resurssit kaikkien kiinteistöistä tulevien hälytysten vastaanottoa varten. Tämä tarkoittaa, että kohteen valvomo-ohjelmiston on

kyettävä käsittelemään usean eri järjestelmän antamat hälytykset ja näyttämään ne myös tarvittaessa alueen karttapohjalla.

Valvontakohteesta saakka tiedonsiirtojärjestelmän on oltava varmennettu, jotta mahdollisten tietoliikennekatkosten vaikutukset saadaan minimoitua. Tämä tarkoittaa etävalvomossa myös kahdennettua asiakas-ohjelmistoa[7]. Tällä toiminnalla saadaan toisen asiakas-koneen kautta hoidettua operatiivinen toiminta toisen ollessa varakoneena ja toisaalta siinä voidaan näyttää kohteiden kuvat ja karttapohjat, joita tarvitaan useimmin tai tilanteen mukaan valitut pohjat. Kameravalvontajärjestelmien osalta keskitetyn etävalvomon tekniikka voi olla esim. seuraavanlaista.

**Monitorit,** jotka on liitetty asiakaskone 1:een esim. neljän näytön (19” – 22”) avulla. Näissä monitoreissa voi olla näkymänä esim. hälytysnäkymäkohteittain, käsiteltävän hälytyksen kohdetiedot, käsiteltävän hälytyskohteen kuva ja käsiteltävän kohteen karttapohjat. Asiakaskoneella 2, jossa esim. kaksi isoa näyttöä (32” tai suurempi) voidaan näyttää etäkohteiden tietoa siten, että esim. näytöllä on karttapohja ja kohteesta neljä kuvaa, jotka liittyvät kohteesta tulleeseen hälytykseen (esim. portit) [7].

**Operatiivinen toiminta** etävalvomoissa tapahtuu TCP/IP-turvaverkon kautta sopivalla valvomo-ohjelmistolla, jolla hallitaan tulevat hälytykset, kuvat ja tarvittavat karttapohjat. Tämän TCP/IP-pohjaisen valvomon kiistattomana etuna on sen sijoitettavuus ja sen käyttöönotto, koska se voidaan helposti siirtää tilanteen ja toiminnan vaatiessa paikasta toiseen. Tällaisen laitteiston kustannukset ovat vain murto-osa videovaihdepohjaisen järjestelmän kustannuksista. Mahdollisissa valvomotoiminnan siirtotapauksissa käyttöönotto kestää vain murto-osan videovaihdepohjaisen valvomon käyttöönotosta[7].

Tällainen valvomo-ohjelmisto tarvitsee toimiakseen mieluimmin 4 Mbit/s tai suuremman kaistan. Tällä kapasiteetilla pystytään ottamaan vastaan kohteiden hälytystietoja, kuvia ja tarvittaessa ohjaamaan kohteen kameroja. Kameraohjaus toteutetaan vain yhtä kameraa kerrallaan ohjaamalla. Pääperiaatteena voidaan pitää, että jokaisesta valvontakohteesta pitää voida ottaa tarvittaessa neljä – kahdeksan samanaikaista kuvaa keskitettyyn valvomoon.

**Tiedonsiirtoverkko** etävalvomon ja valvontakohteen välillä pitää mitoittaa oikein vastaamaan kohteiden välistä liikennöintiä. Normaalisti hajautetussa tallennusjärjestelmäs-

sä ja videovaihteiden välisessä ns. satelliittiyhteydessä riittää 4 Mbit/s verkkoyhteys. Tiedonsiirtoverkko on varmennettava vähintään kahdella erillisellä verkkoyhteydellä, jota varmistetaan vielä GPRS-yhteyksillä. GPRS-yhteyksissä siirretään vain palo- ja rikosilmoitinjärjestelmän hälytystietoa, ei siis kuvaa.

### 8.3.3 Muiden turvallisuusjärjestelmien integrointimahdollisuudet

Keskitetyn valvomon kaikki turvallisuusjärjestelmän osa-alueet voidaan integroida samaan järjestelmään, jolloin laitteiden kirjo ei kasva suureksi. Tällainen keskitetty hälytysten vastaanotto-ohjelma on esim. Interview (IVA). Rikos-, paloilmoitin- ja muiden kiinteistöjärjestelmien hälytykset voidaan ohjata esim. IVA-järjestelmään, jossa ne voidaan ottaa vastaan, käsitellä, suorittaa jatkohälytykset, kommentoida ja arkistoida. Paloilmoitinjärjestelmä laitteiden huollon, testausten ja muun toiminnan takia on hyvä olla erillinen hallintaohjelmisto, millä voidaan suorittaa yksittäisten silmukoiden irtikytkentöjä esim. tulitöiden tai paloharjoitusten ajaksi. Kameravalvontajärjestelmä on oma kokonaisuutensa varsinkin silloin, kun on useita valvottavia etäkohteita ja näissä kohteissa on runsaasti kameroita. Rikosilmoitinjärjestelmän hälytysten vastaanotto-ohjelmaan voidaan laittaa opastuskenttiä, joita voi hyödyntää kameravalvontajärjestelmän kanssa. Kulunvalvontajärjestelmä toimii omana kokonaisuutena, sillä keskitetyn valvomon pääasialliset tehtävät liittyvät yleensä kadonneiden etälukutagien ”kuoletukseen” virka-ajan ulkopuolella.

Porttipuhelinjärjestelmät voidaan myös liittää keskitettyyn valvomon valvomoon. Rekisteritunnistusjärjestelmätkin voidaan hallinnoida etähallintaohjelmistojen avulla keskitetystä valvomosta.

## 8.4 Etäkohteiden valvonta normaalioloissa

Keskitetty valvomo pystyy normaalioloissa vastaamaan usean etäkohteen valvonnasta. Päivittäisten arkirutiinien hoidosta vastaavat eri turvallisuusjärjestelmät automaattisesti esim. ajoneuvontunnistus- ja rekisterintunnistusjärjestelmä, kulunvalvonta-, paloilmoitin-, rikosilmoitin- ja työajanseurantajärjestelmä. Kameravalvontajärjestelmä seuraa ja tallentaa etäkohteiden kameroiden avulla ne kriittiset paikat, joihin ne on kiinteästi asennettu tai ohjelmallisesti ohjattu. Toiminta keskitetyssä valvomossa vilkastuu, kun toiminta etäkohteissa työpäivän päätyttyä hiljenee. Kaikkien järjestelmien hälytykset, ohjauk-

set, päivitykset ja muutokset siirtyvät keskitetyn valvomon vastuulle. Toiminnan pitää jatkua vastaavanlaisena kuten päivälläkin, sillä turvallisuusjärjestelmien toiminta ei ole riippuvainen valvomon sijainnista. Kameravalvontajärjestelmällä suoritetaan ne samat valvontakierrokset, kuten aikaisemmin paikallisvalvomostakin. Toiminnallisesti kaiken pitää sujua kuten paikallisvalvomonkin tekemänä. Kaiken toiminnan lähtökohtana on toimiva verkkoyhteys.

### 8.5 Etäkohteiden valvonta poikkeusoloissa

Keskitetty valvomo pystyy hoitaan myös poikkeusolojen valvontaa niin kauan kun verkkoyhteydet toimivat. Poikkeusolot eivät tarkoita tässä kohdassa sodanuhkaa tai – aikaa. Poikkeusolot ovat normaalista poikkeavaa tilanne, jonka yrityksen turvallisuusjohto on määrittänyt. Tällaisia voivat olla esim. tulipalo, lakko, mielenosoitus, vakava onnettomuus tai työtapaturma, kuolema jne.

Tällaisissa tapauksissa kohteissa on poikkeusolojen toimintasuunnitelma, jonka mukaan keskitetty valvomo hälytyttää ne avainhenkilöt paikalle, jotka alkavat johtaa toimintaa paikanpäällä. Tähän poikkeusolojen toimintasuunnitelmaan kuuluu olennaisena osana paikallisen vartiohenkilöstön hälyttäminen. Toimintaa voidaan jakaa keskitetyn valvomon ja paikallisen vartiohenkilöstön kesken esim. seuraavalla tavalla: keskitetyn valvomon henkilöstö hoitaa niitä turvallisuusjärjestelmiä etänä mitä pystyvät ja informoivat havaitsemista poikkeamista paikalliselle vartiohenkilöstölle.

Poikkeusoloissa myös paikallisissa vartioiden käytössä olevissa ajoneuvoissa voi olla järjestelmään liitetyt kannettavat tietokoneet ja esim. WLAN, 3G tai @450-yhteydet, jolloin saadaan valvomotoiminnot siirrettyä lähemmäs esim. onnettomuuspaikkaa.

## 9. Johtopäätökset

Kameravalvontajärjestelmä kehitys viimeisen kymmenen vuoden aikana on ollut hyvin nopeaa. Tästä hyvänä esimerkkinä on kokonaan uuden kamerajärjestelmän kehittyminen eli IP-kamerat. Toisena merkittävänä tekijänä on ollut tiedonsiirtoverkkojen yleistyminen ja niiden kapasiteetin kasvu ja tietysti hintatason laskeminen. Tiedonsiirtoverkkojen kapasiteetti ja niiden saatavuus ei rajoita millään puolella Suomea valvomotoiminto-

jen keskittämistä nyt eikä tulevaisuudessa. Tulevaisuudessa kameravalvontajärjestelmät käyttävät yhä kasvavassa määrin hyväkseen digitaalitekniikan antamia lähes rajattomia mahdollisuuksia käsitellä, siirtää, muokata ja tallentaa kuvaa. Kuvaa voidaan siirtää pakkaustekniikoiden kehittymisen seurauksena tulevaisuudessa lähes laitteeseen kuin laitteeseen. Tällaisia laitteita voivat olla vaikka esim. kämmenmikrot, puhelimet, navigaattorit jne. Tästä on seurauksena se, että entistä paremmin voidaan hyödyntää kriisien, onnettomuuksien ja muiden normaalista poikkeavien tilanteiden johtamisessa reaaliaikaista tilannekuvaa kohteesta.

IP-kameratekniikka, kuvantallennustekniikka ja verkkotekniikka kehittyvät jatkuvasti huimasti eteenpäin. Tämä mahdollistaa sen, että yksittäisillä kameroilla voidaan valvoa yhä suurempia alueita, joista voidaan tunnistaa henkilöitä ja esim. ajoneuvojenrekisterinumeroita. Tulevaisuuden kamerat ovat kokoluokaltaan jopa 30 – 40 Mpix. Tämän kokoluokan kameroiden kuvaa voidaan suurentaa jopa 100 kertaiseksi verraten alkuperäiseen kuvaan. Nämä kamerat vaativat oman noin 100 Mbit/s tai jopa 1 Gbit/s verkkoliittymän. Tämä edellä kerrottu määrä vastaa tavallisia analogisia kameroita (erottelutarkkuus 700 x 500 pikseliä) noin 85 – 100 kappaletta, jotta saavutettaisiin vastaava erottelutarkkuus ja valvonta-ala. Todennäköisesti kameramäärän muutoksen vaikutus suunnitteluun, asennuksen, huollon ja ylläpidon kustannuksiin on IP-kameratekniikalle erittäin edullinen.

Kuvantallennustekniikalle tällainen valtavan kokoluokan kameroiden tulo markkinoille pakottaa kehittämään niin tallennuskapasiteettia kuin myös kuvatallenteiden etsintäparametreja, jotta kulloinkin tarvittavat kuvatallenteet löytyisivät riittävän nopeasti. Hahmontunnistustekniikan kehittyvät tietotekniikan kehityksen myötä ja tuulevat helpottamaan niin tallennuskapasiteetin tarpeita kuin myös tallenteiden etsinnässä.

Valvomo-ohjelmistotekniikat kehittyvät tulevaisuudessa entistä monipuolisemmiksi ja automaattisemmiksi siten, että ne antavat kohteesta kuvan kanssa runsaasti myös muuta informaatiota esim. tuulensuuntaa ja – nopeutta, lämpötilaa, kosteutta, kameran suuntaa kompassisuuntana, havaitun kohteen etäisyyttä jne. Nämä tiedot tietenkin auttavat niissä poikkeusoloissa, jossa jokainen sekunti on ratkaiseva.

# 10. Yhteenveto

Tämän hetken Suomessa eletään kameravalvontajärjestelmien murroskautta, jossa uusi IP-kameratekniikka, tiedonsiirtoverkot, hajautetut tallennusjärjestelmät ja keskitetyt valvomoratkaisut ovat keskeisessä asemassa niin kaupanalan, yksityisen teollisuuden, julkishallinnon kuin viranomaistahojenkin keskuudessa, kun suunnitellaan tulevaisuuden turvallisuusratkaisuja. Kaikilla toimijoilla on samana yhteisenä päämääränä kustannusten säästö turvallisuustasoa laskematta.

On sanomattakin selvää, että kaikkea turvallisuustoimintaa ei voi toteuttaa etänä tietoverkkojen kautta vaan tarvitaan yhä myös läsnä olevaa turvallisuushenkilöstöä monissa erinäisissä tehtävissä. Turvallisuushenkilöstön tehtäviä ja muita kohteen toimintoja voidaan kyllä yhdistää, kunhan eri toimijoiden mieli ja ajatukset ovat kypsät tähän toimintaan.

Kameravalvontajärjestelmien rakentaminen jatkuu edelleen vilkkaana ja järjestelmiä rakennetaan niin perinteisen analogisen kameratekniikan kuin IP-kameratekniikankin laitteilla kulloisenkin tarpeen ja tilanteen mukaan. Oikein suunnitelluilla ja asennetuilla kameravalvontajärjestelmillä saadaan tehokkuutta erilaisiin palveluihin ja prosesseihin, ilkivallan ja anastusten teon kynnys nousee ja tapahtumien selvittäminen jälkikäteen paranee huomattavasti.

Mietittäessä kumpi on parempi keskitetty vai hajautettu valvomoratkaisu, niin voidaan todeta, että molemmissa on omat vahvuutensa. Nopeasti kehittyvän tekniikan ja muuttuvat turvatarpeet vaikuttavat keskitetyn ja hajautetun järjestelmän välisiin painotuksiin ja valintakriteereihin jatkuvasti. Suoraa vastausta kysymykseen; kumpi on käyttökelpoisempi nyt tai tulevaisuudessa, ei ole. Kameravalvontajärjestelmä on syytä aina suunnitella kulloisenkin tarpeen ja saatavilla olevien komponenttien ja tekniikoiden mukaan siten, että nykyisiin asetettuihin valvontavaatimuksiin vastataan järkevin kustannuksin. Korkealaatuisen toteutuksen tunnistaa siitä, että järjestelmä on myöhemmin helppo päivittää, laajentaa ja sen elinkaari on pitkä. Tutkielma pyrkii antamaan lukijalle näkökulmia ja työkaluja tähän tavoitteeseen pääsemiseksi.

## 11. Sanasto ja kuvauksia teknisistä termeistä

**Multiplekseri** on laite, johon liitetään analogisia kameroita koaksiaalikaapelilla. Laitteen tehtävänä on vaihtaa monitorille liitettyjen kameroiden kuvia tietyllä kierrolla. Kameroita siihen voidaan liittää laitteen koosta riippuen 6 – 16 kappaletta. Multiplekseristä voidaan ottaa kamerakuvat monitoreille (2 kappaletta), monitoreihin voidaan ohjelmoida kuvakierrot. Multiplekserin kautta on toteutettu myös kuvien tallennus VHS-nauhureille tai yksi kanavaisille digitaalitallentimille

**Videovaihde** on laite, johon voidaan liittää analogisia kameroita koaksiaalikaapelilla. Kameroita voidaan liittää laitteen koosta riippuen 6 – 1 000 kappaletta. Videovaihdetta hallitaan erillisellä käyttölaitteella. Videovaihteesta voidaan ottaa liitetyt kamerakuvat monitoreille, joita voidaan liittää 2 – 65 kappaletta. Monitoreihin voidaan ohjelmoida halutut kuvakierrot.

**CCD-kenno** [10] (engl. *Charge-Coupled Device*) on valoherkkä kenno, joita käytetään muiden muassa video- ja digitaalikameroissa, kuvanlukijoissa ja kaukoputkissa valon tai infrapunasäteilyn muuntamiseksi digitaaliseksi signaaliksi. Kennon valoherkät fotodiodit eivät näe värejä, vaan ne muodostavat kohteesta säteilyn voimakkuuden pohjalta harmaasävykuvan. Värit syntyvät valoherkkien diodien päällä olevista värisuotimista. Värisuotimet ovat yleensä punainen, vihreä ja sininen.

**DSP-tekniikka** [10] on lyhenne sanoista **D**igital **S**ignal **P**rosesing, joka on suomeksi digitaalinen signaalinkäsittely.

**CIF** [10] on lyhenne sanoista **C**ommon **I**ntermediate **F**ormat, joka 2000-luvun taitteessa tarkoitti videoneuvottelutyökaluja. Nykyään sillä tarkoitetaan resoluutiota 352 x 288 PAL 352 x 240 NTSC. CIF on neljännes normaalin television resoluutiosta, joka tunnetaan myös nimellä D1.

**CAT5 / CAT6** [10] on kierretty parikaapeli, jossa käytetään toistensa ympäri kierrettyjä johdinpareja häiriöiden vähentämiseksi. Parikaapeleita voidaan käyttää muun muassa Token Ring-, puhelin-, Ethernet-, ISDN- ja ATM-yhteyksiin. Yleisin liitintyyppi kierretylle parikaapeleille lähiverkossa on RJ-45. CAT5 kaapelilla kaistanleveys on 100MHz. CAT6 on käytännössä sama kuin CAT5, mutta testausstandardit ovat toiset. Jotta Gigabit Et-

hernet saadaan luotettavasti toimimaan, käytetään CAT6-kaapelia. CAT6 kaapelilla kaistanleveys on 250MHz. Tämä on vuodesta 2002 yleisin Suomessa asennettu.

**POE** [10] on lyhenne sanoista **P**ower **O**ver **E**thernet, joka tarkoittaa sitä, että virransyöttö tapahtuu erilaisille päätelaitteille Ethernet-kaapelin kautta samanaikaisesti tiedonsiirron kanssa. POE-tekniikan yleisimpiä käyttökohteita ovat mm. VoIP-puhelinjärjestelmät, Ethernet-kytkimet sekä IP-turvakamerat. PoE-tekniikan avulla saavutetaan kustannus-säästöjä kohteissa, joissa muuten jouduttaisiin huolehtimaan sähkönsyötöstä erikseen.

**CMOS-kenno** [10] on digitaalikameroissa käytettävän valoherkän kennon tyyppi, joka on alkanut syrjäyttää vanhempaa CCD-kennona. CCD-kennoja käytetään yhä edelleen paremmissa kameroissa. CMOS-kennossa jokaisessa pikselissä itsessään tehdään muunnos varauksesta jännitteeksi sekä signaalin vahvistus, jolloin varausta ei tarvitse siirtää kennopiirillä mihinkään. Näin CMOS-kennoilla päästään yleensä pienempään virrankulutukseen kuin CCD-kennoilla. Useinmiten AD-muunnos tehdään CMOS kennopiirillä, jolloin kamerassa tarvitaan vähemmän muita piirejä.

## 12. Lähteet

Haastattelut:

1. Hirvonen, Jukka — ISS Security Oy, Avainasiakaspäällikkö
   IP-kamera- ja tallennintekniikka
2. Jokinen, Sampo — ISS Security Oy, Tuotekehityspäällikkö
   Turvaverkkoratkaisut
3. Kaikkonen, Juha — ASAN Security Technologies Oy, Asiakaspalvelujohtaja
   IP-kameratekniikka ja valvomo-ohjelmisto, ASAN ASC
4. Kesti, Mikko — ISS Security Oy, Palvelujohtaja
   Vartiointipalvelujen kustannuslaskenta
5. Lampela, Pekka — Sick Oy, Aluemyyntipäällikkö
   Laser-skannerit
6. Lankinen, Ari — Bosch Security Systems, Avainasiakaspäällikkö
   Analogi- ja IP-kamerat
7. Määttä, Marko — ISS Security Oy, Aluepäällikkö
   Turvallisuusvalvomo
8. Rajanen, Timo — ISS Security Oy, Asiakaspäällikkö
   Analogi- ja IP-kameratekniikat
9. Ylä-Kojola, Marco — Mirasys Oy, Myyntijohtaja
   Valvomo-ohjelmisto, RMC

Kirjalliset lähteet:

10. Sivusto — Wikipedia hakusanoilla ”CCD-kenno, DSP- tekniikka, CIF, CAT5/CAT6, POE, CMOS-kenno ja TCP/IP”
11. Sivusto — www.finlex.fi

## 13. Liitteet

Liite 1: Kameravalvontajärjestelmään liittyvät keskeisimmät lainsäädännöt

Liite 2: Laser-skannerin käyttösovellutuksia

Liite 3: IP-kameroiden maksimiverkkokuormitus, Laskelma

14. Liite 1; Kameravalvontaan liittyvät keskeisemmät lainsäädännön kohdat

Seuraavassa lyhyesti em. lakien tärkeimmät kohdat, joiden mukaan kameravalvontajärjestelmä pitää olla toteutettu.

***Henkilötietolaki 22.4.1999/523*** [11]

***2 luku***

*Henkilötietojen käsittelyä koskevat yleiset periaatteet*

**6 §**

**Henkilötietojen käsittelyn suunnittelu**

*Henkilötietojen käsittelyn tulee olla asiallisesti perusteltua rekisterinpitäjän toiminnan kannalta. Henkilötietojen käsittelyn tarkoitukset sekä se, mistä henkilötiedot säännönmukaisesti hankitaan ja mihin niitä säännönmukaisesti luovutetaan, on määriteltävä ennen henkilötietojen keräämistä tai muodostamista henkilörekisteriksi. Henkilötietojen käsittelyn tarkoitus tulee määritellä siten, että siitä ilmenee, minkälaisten rekisterinpitäjän tehtävien hoitamiseksi henkilötietoja käsitellään.*

**7 §**

**Käyttötarkoitussidonnaisuus**

*Henkilötietoja saa käyttää tai muutoin käsitellä vain tavalla, joka ei ole yhteensopimaton 6 §:ssä tarkoitettujen käsittelyn tarkoitusten kanssa. Myöhempää henkilötietojen käsittelyä historiallista tutkimusta taikka tieteellistä tai tilastotarkoitusta varten ei pidetä yhteensopimattomana alkuperäisten käsittelyn tarkoitusten kanssa.*

**10 §**

**Rekisteriseloste**

*Rekisterinpitäjän on laadittava henkilörekisteristä rekisteriseloste, josta ilmenee:*
*1) rekisterinpitäjän ja tarvittaessa tämän edustajan nimi ja yhteystiedot;*
*2) henkilötietojen käsittelyn tarkoitus;*
*3) kuvaus rekisteröityjen ryhmästä tai ryhmistä ja näihin liittyvistä tiedoista tai tietoryhmistä;*
*4) mihin tietoja säännönmukaisesti luovutetaan ja siirretäänkö tietoja Euroopan unionin tai Euroopan talousalueen ulkopuolelle; sekä*
*5) kuvaus rekisterin suojauksen periaatteista.*

*Rekisterinpitäjän on pidettävä rekisteriseloste jokaisen saatavilla. Tästä velvollisuudesta voidaan poiketa, jos se on välttämätöntä valtion turvallisuuden, puolustuksen tai yleisen järjestyksen ja turvallisuuden vuoksi, rikosten ehkäisemiseksi tai selvittämiseksi taikka verotukseen tai julkiseen talouteen liittyvän valvontatehtävän vuoksi.*

***Rikoslaki 19.12.1889/39*** [11]

***24 luku (9.6.2000/531)***
***Yksityisyyden, rauhan ja kunnian loukkaamisesta***

***3 § (15.7.2005/585)***
***Julkisrauhan rikkominen***
*Joka oikeudettomasti*
*1) tunkeutuu taikka menee salaa tai toista harhauttaen virastoon, liikehuoneistoon, toimistoon, tuotantolaitokseen, kokoustilaan taikka muuhun vastaavaan huoneistoon tai rakennukseen tai sellaisen rakennuksen aidatulle piha-alueelle taikka kasarmialueelle tai muulle puolustusvoimien tai rajavartiolaitoksen käytössä olevalle alueelle, jolla liikkuminen on asianomaisen viranomaisen päätöksellä kielletty, taikka*
*2) kätkeytyy tai jää 1 kohdassa tarkoitettuun paikkaan, on tuomittava julkisrauhan rikkomisesta sakkoon tai vankeuteen enintään kuudeksi kuukaudeksi.*
*Julkisrauhan rikkomisena ei kuitenkaan pidetä tekoa, josta on aiheutunut ainoastaan vähäinen haitta*.

***6 § (9.6.2000/531)***
***Salakatselu***
*Joka oikeudettomasti teknisellä laitteella katselee tai kuvaa*
*1) kotirauhan suojaamassa paikassa taikka käymälässä, pukeutumistilassa tai muussa vastaavassa paikassa oleskelevaa henkilöä taikka*
*2) yleisöltä suljetussa 3 §:ssä tarkoitetussa rakennuksessa, huoneistossa tai aidatulla piha-alueella oleskelevaa henkilöä tämän yksityisyyttä loukaten, on tuomittava salakatselusta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.*
*Yritys on rangaistava.*

***Laki yksityisyyden suojasta työelämässä 13.8.2004/759*** [11]

5 luku

Kameravalvonta työpaikalla

***16 §***
***Kameravalvonnan edellytykset***
*Työnantaja saa toteuttaa jatkuvasti kuvaa välittävän tai kuvaa tallentavan teknisen laitteen käyttöön perustuvaa valvontaa (kameravalvonta) käytössään olevissa tiloissa työntekijöiden ja muiden tiloissa oleskelevien henkilökohtaisen turvallisuuden varmistamiseksi, omaisuuden suojaamiseksi tai tuotantoprosessien asianmukaisen toiminnan valvomiseksi sekä turvallisuutta, omaisuutta tai tuotantoprosessia vaarantavien tilanteiden ennaltaehkäisemiseksi tai selvittämiseksi. Kameravalvontaa ei kuitenkaan saa käyttää tietyn työntekijän tai tiettyjen työntekijöiden tarkkailuun työpaikalla. Käymälässä, pukeutumistilassa tai muussa vastaavassa paikassa tai muissa henkilöstötiloissa taikka työntekijöiden henkilökohtaiseen käyttöön osoitetussa työhuoneessa ei myöskään saa olla kameravalvontaa.*

***17 §***

***Avoimuus kameravalvontaa toteutettaessa***

*Työnantajan on kameravalvontaa suunnitellessaan ja toteuttaessaan pidettävä huolta siitä, että:*

*1) ennen kameravalvonnan käyttöönottamista selvitetään työntekijöiden yksityisyyteen vähemmän puuttuvien muiden keinojen käyttömahdollisuudet;*

*2) työntekijän yksityisyyteen ei puututa enempää kuin on välttämätöntä toimenpiteiden tarkoituksen saavuttamiseksi;*

*3) valvonnalla saatujen henkilöitä koskevien tallenteiden käyttö ja niiden muu käsittely suunnitellaan ja toteutetaan ottaen huomioon, mitä henkilötietolain 5–7, 10 ja 32–34 §:ssä säädetään, riippumatta siitä, muodostavatko tallenteet mainitussa laissa tarkoitetun henkilörekisterin;*

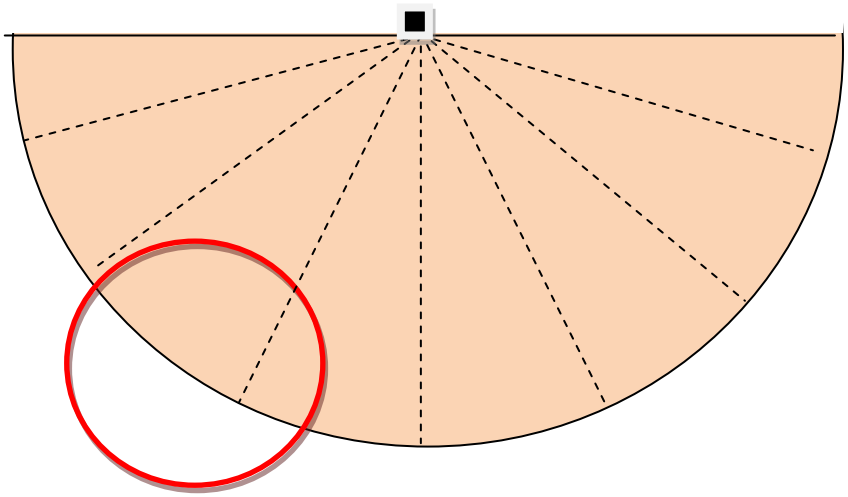
*4) tallenteita käytetään vain niihin tarkoituksiin, joita varten tarkkailua on suoritettu;*

*5) työntekijöille tiedotetaan 21 §:ssä tarkoitetun yhteistoiminta- tai kuulemismenettelyn jälkeen kameravalvonnan alkamisesta, toteuttamisesta ja siitä, miten ja missä tilanteissa mahdollisia tallenteita käytetään sekä 16 §:n 2 momentin tarkoittamissa tilanteissa kameroiden sijainnista; ja*

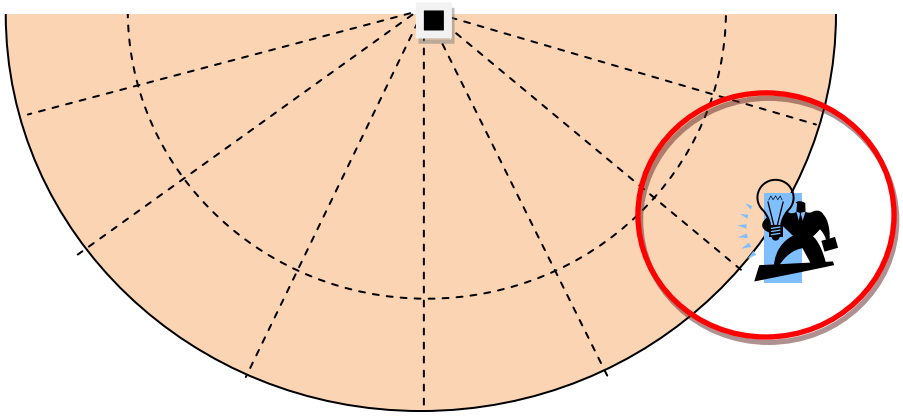
*6) kameravalvonnasta ja sen toteuttamistavasta ilmoitetaan näkyvällä tavalla niissä tiloissa, joihin kamerat on sijoitettu.*

15. Liite 2; Laser-skannerin käytännön sovellutukset

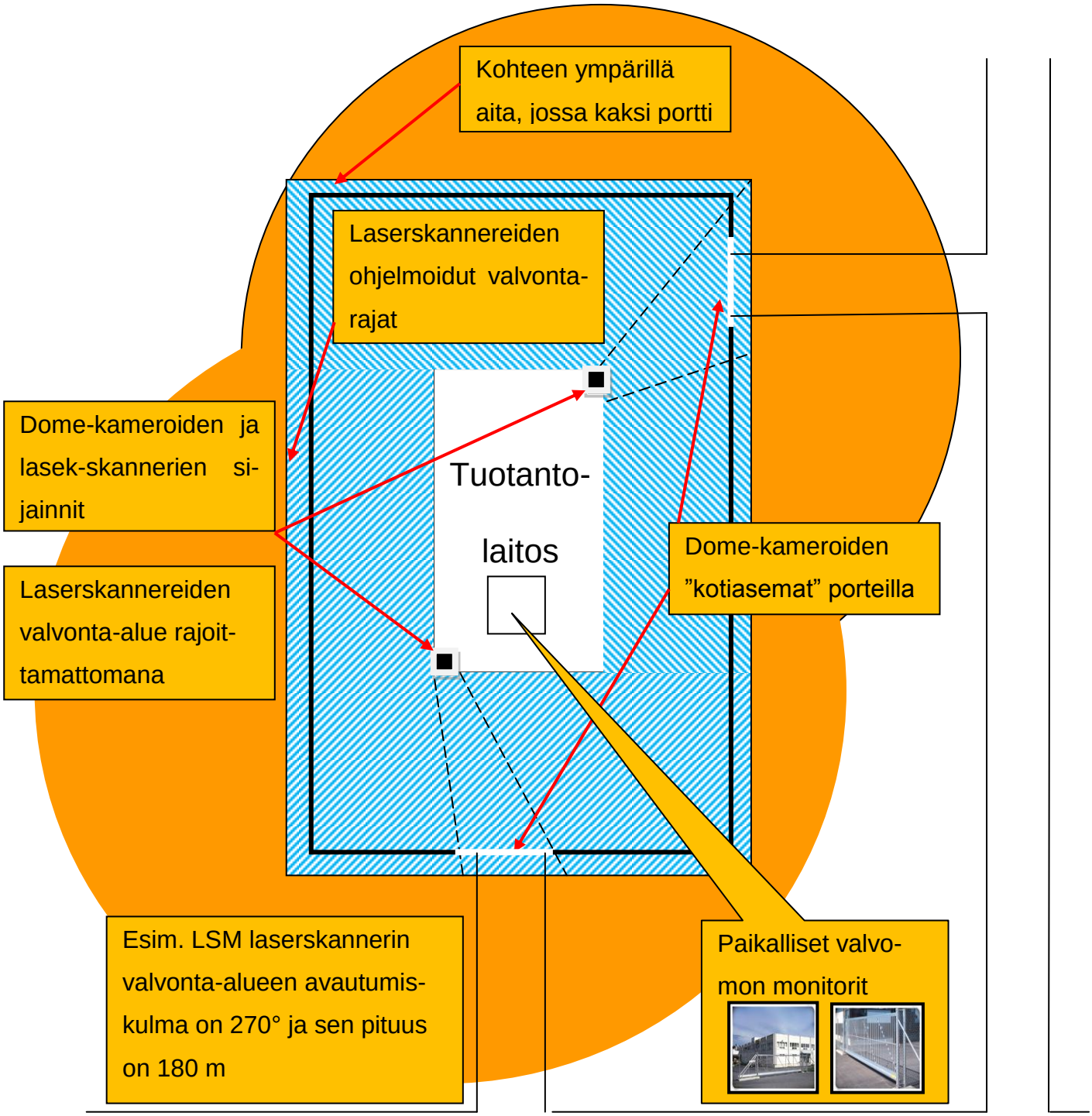
Alhaalla olevassa kuvassa laser-skannerin ”näkökenttä”. kentän voi sektoroida lähes haluamallaan tavalla. Domekameran ”kotiasento” on ohjelmoitu rengastettuun sektorin osaan



Alhaalla olevassa kuvassa toiseen laser-skannerin ohjelmoituun valvontakenttään tulee häiriö, joka aiheuttaa dome-kameran kääntymisen häiriön aiheuttaneeseen sektoriin

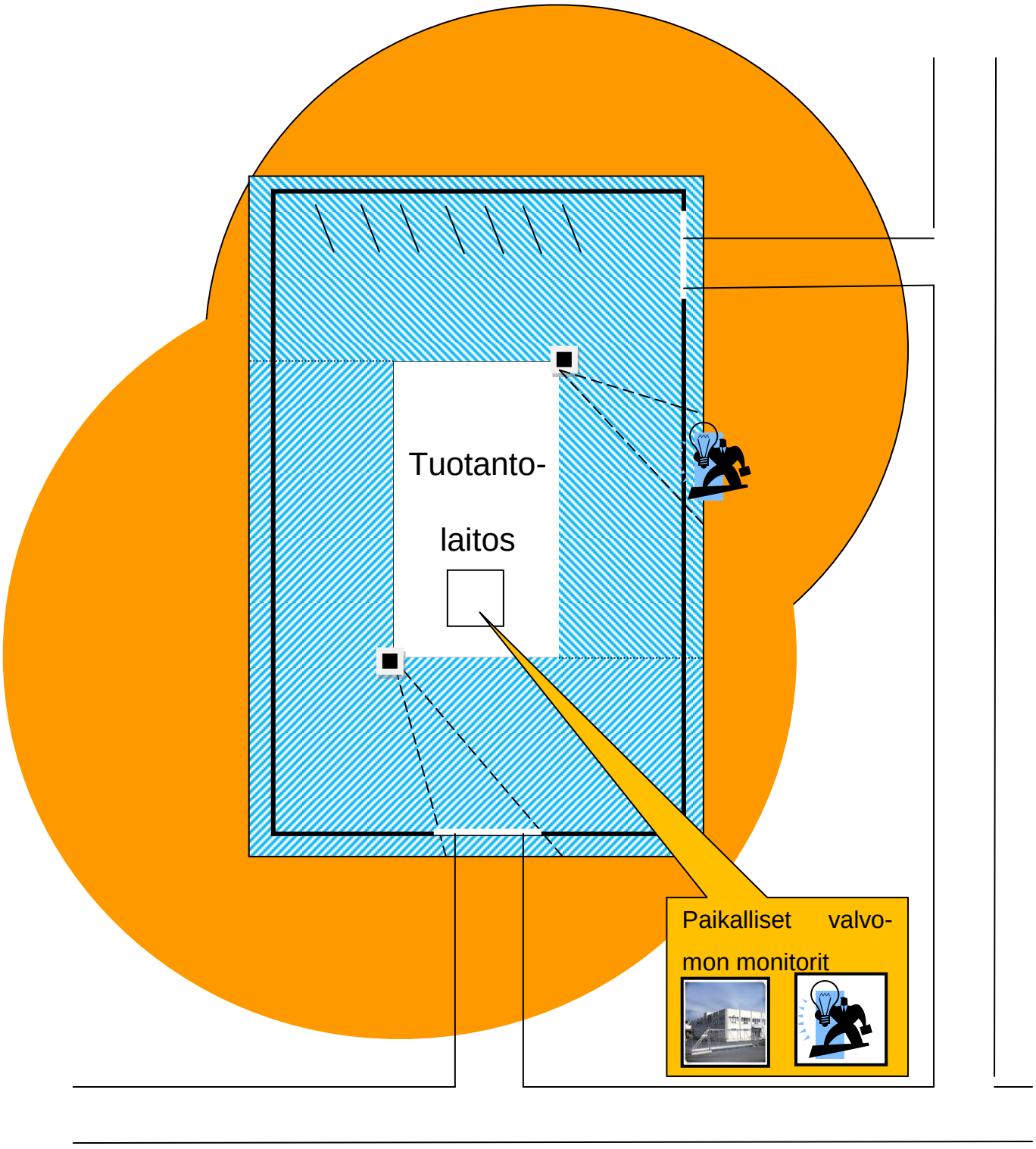


e

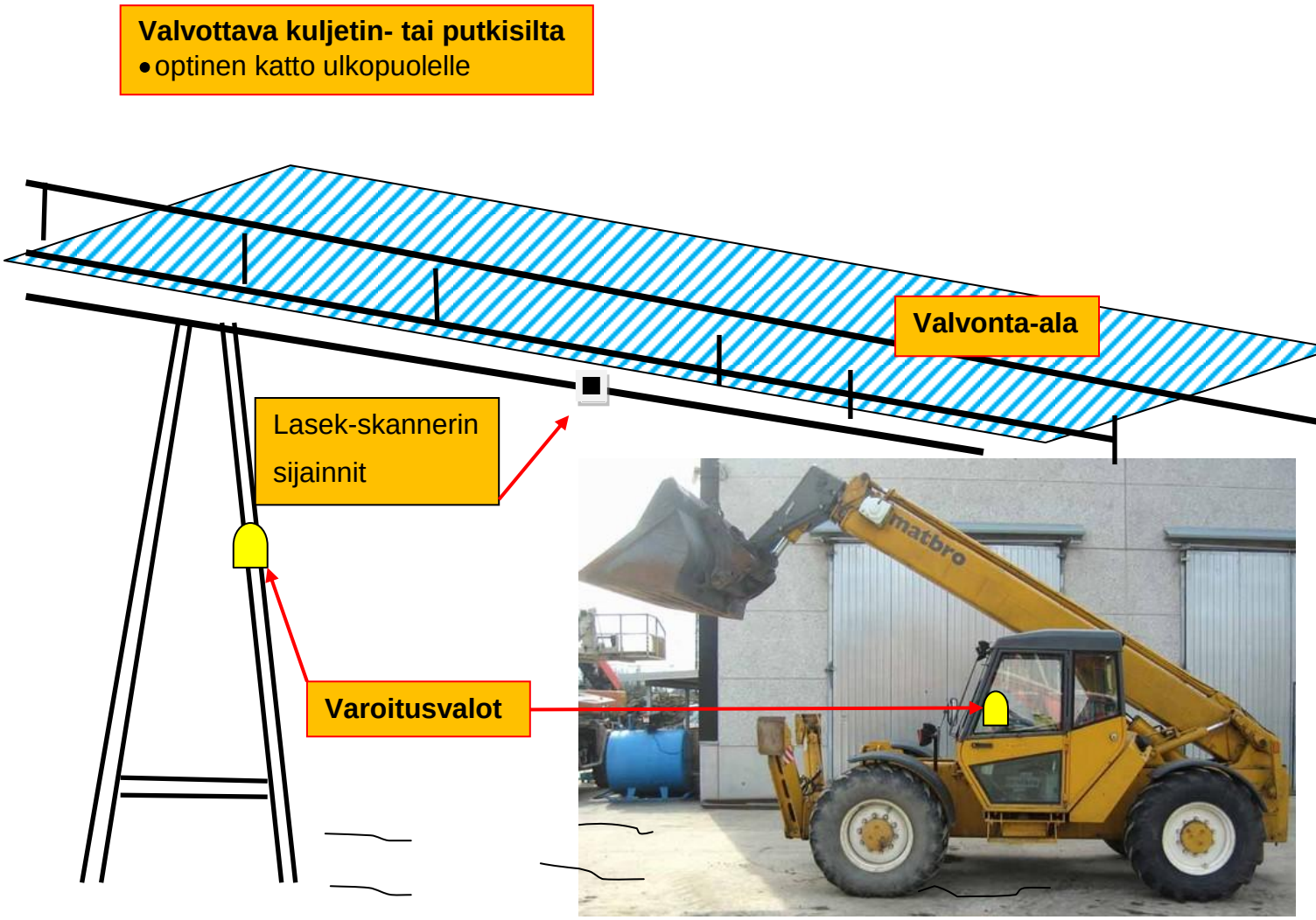



Ylhäällä olevassa kuvassa kahdella laserskannerilla ja kahdella dome-kameralla valvot-tu teollisuusalueen kehävalvonta.

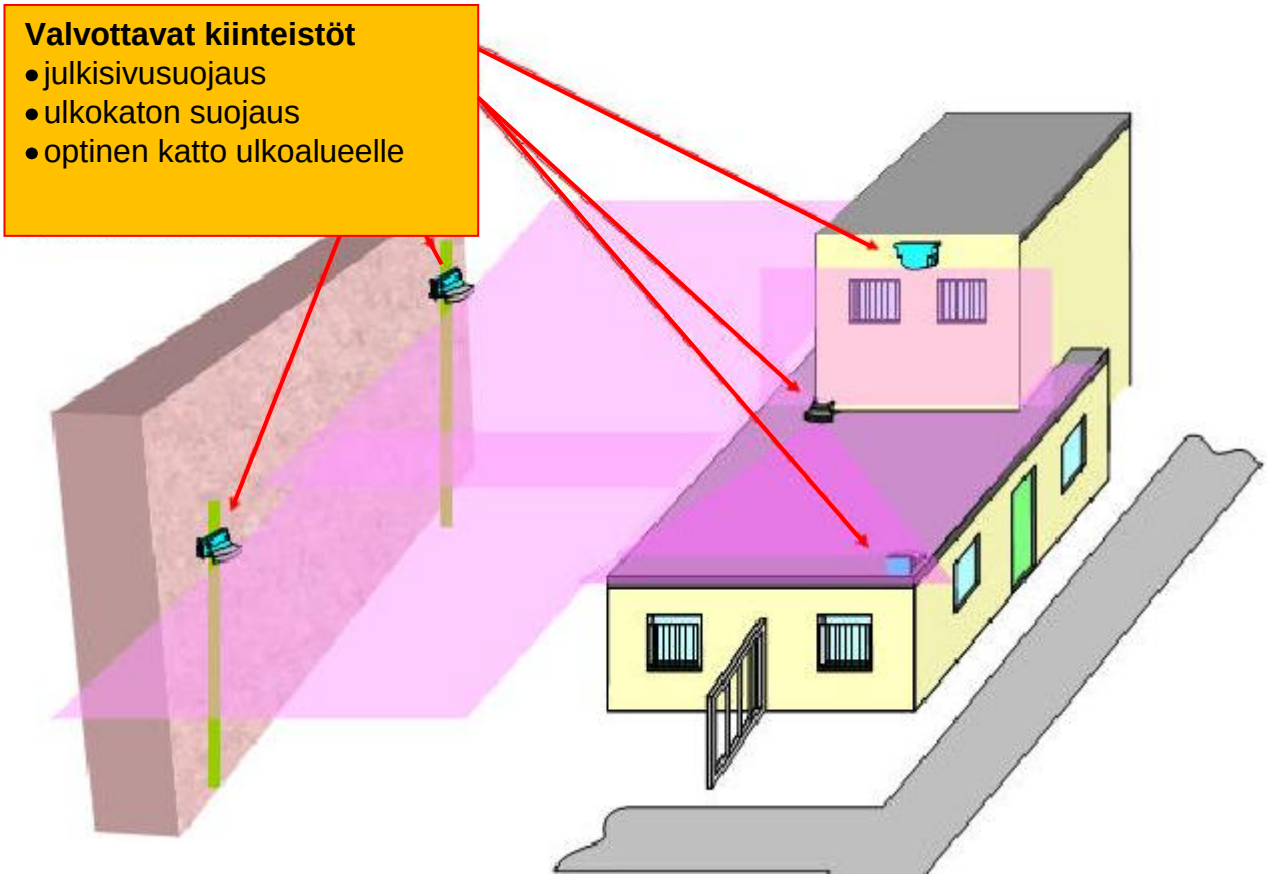
f



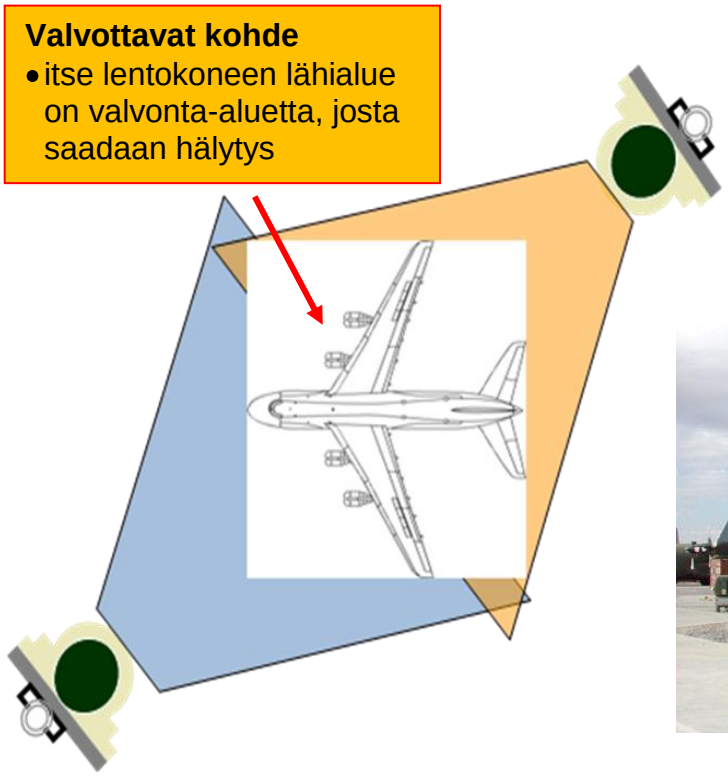

Yllä olevassa kuvassa toisen laser-skannerin ohjelmoituun valvontakenttään tulee häiriö, joka aiheuttaa toisen dome-kameran kääntymisen häiriön aiheuttaneeseen kohtaan. Tieto mahdollisesta ”tunkeutumisesta” tulee jo siinä vaiheessa, kun kohde on vielä tehdasalueen aidan ulkopuolella. Vartiohenkilöstölle saadaan tällöin enemmän toiminta-aikaa ja mahdollisen kohteen tunnistaminen kameralla/kameroiden avulla paranee.




Yllä olevassa kuvassa laser-skannerin eräs käyttösovellutus ylätason eli korkeuden ylärajan tunnistimena ja hälytystiedon välittäjänä varoitusmajakoille / sireeneille. Sama tieto lähetetään myös langattomasti työkoneen hyttiin, jolloin kuljettaja huomaa tapahtumassa olevan törmäyksen. Kuljettajalle jää aikaa toimia, jolloin vältytään koneen ja putki- tai kuljetinsillan vauriolta. Työkoneessa hälytys näytetään varoitusmajakalla.




Yllä olevassa kuvassa laser-skannerin eräs käyttösovellutus ylätason eli korkeuden ylärajan tunnistimena, kattotasoja ja seinäpintojen valvonnassa. Sovellutuskohteita löytyy esim. vankilaympäristöistä.




Yllä olevassa kuvassa lentokoneen suojaaminen kahdella laser-skannerilla. Kohteen valvonta-alueelle meno aiheuttaa hälytyksen.

## 16. Liite 3; Laskelma maksimi verkkokuormituksesta

Seuraavassa kaksi esimerkki laskelmaa käytettäessä erikokoista kuvaa kameroissa. Esimerkki 1. Käytetään **CIF (kts. sivu 11 kuva)** kokoista kuvaa (352 x 288), liiketunnistus tapahtuu kamerassa.

- Yksi kuva on 15 kB eli yksi kuva sekunnissa aiheuttaa kuromaa verkkoon
  15 kB/s = 15 x 1,024 x 8 bit/byte = **122,9 kbit/s**
- Halutaan katsoa kuvaa 3 fps ja tallentaa 2 fps, eli yhteensä 5 fps
  5 fps = 5 x 122,9kbit/s = **614,4kbit/s**
- Näitä kameroita on käytössä 20 kappaletta, jolloin **maksimikuorma** verkossa on:
  20 x 5 fps = 20 x 122,9 kbit/s x 5 fps = **12,3 Mbit/s**

Esimerkki 2. Käytetään **4CIF (kts. sivu 15 kuva)** kokoista kuvaa (704 x 576), liiketunnistus tapahtuu kamerassa.

- Yksi kuva on 30 kB eli yksi kuva sekunnissa aiheuttaa kuromaa verkkoon
  30 kB/s = 30 x 1,024 x 8 bit/byte = **245,76 kbit/s**
- Halutaan katsoa kuvaa 3 fps ja tallentaa 2 fps, eli yhteensä 5 fps
  5 fps = 5 x 245,76 kbit/s = **1 228,8 kbit/s**
- Näitä kameroita on käytössä 20 kappaletta, jolloin **maksimikuorma** verkossa on:
  20 x 5 fps = 20 x 245,76 kbit/s x 5 fps = **24,6 Mbit/s**